INTERNATIONAL WORKSHOP AGREEMENT

IWA 44

Draft
2024-10-22

Unique Media Identifier (UMId) for distribution channels and brands

DRAFT - Public consultation

Call for comments

(End date: 2024-11-29)

Please **submit your comments (if any) no later than 2024-11-29** via E-Mail to:

gregor.roschkowski@din.de; umid@mediaregistry.org

Please note that **comments will only be accepted using the ISO commenting template**. The ISO commenting template is available for download here.

Please also note that in the ISO commenting template a specific change proposal is mandatory for each comment (in the column "Proposed change") or the comment may not be accepted.

In the 1st column of the commenting template (MB/NC), please indicate the organization/company you are representing. In the 5th column of the commenting template (Type of comment) please indicate the type of comment: "ge = general" or "te = technical" or "ed = editorial".

Warning for Draft

This document is distributed for review and comment. It is subject to change without notice.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Reference number
IWA 44 Draft:2024(E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

International Workshop Agreement IWA 44 was approved at a series of workshops hosted by the German Institute for Standardisation (DIN), in association with Global Media Registry (GMR), held between February 2024 and January 2025.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Unique Media Identifiers (UMId), as covered by this IWA, are a tool to enhance the integrity of the online news ecosystem – among other things, by harmonising and improving the effectiveness of respective signalling along the distribution chain to facilitate content indexation and recommendation by online platforms (e. g. search, streaming and social media). In addition, the deliverables of the IWA can be used by all other stakeholders that engage with mass media and content distribution online, such as providers/operators of advertising technology, and public sector actors (e. g. regulatory authorities).

The functioning of our shared information space depends on digital infrastructure and platforms. Their protocols and algorithmic-driven recommender systems determine how content can be accessed by users online. In order to work properly, these recommender systems require up-to-date criteria by which content is included, promoted or even excluded based upon inclusion lists of trustworthy sources of content, or exclusion lists of bad actors.

The unique key of the UMId will be designed to provide signal transparency and integrity in a neutral way and will be assigned to media outlets (which means all distribution channels and brands of a content provider), so that the industry, regulators, audiences and other stakeholders can unambiguously identify the respective source of information, for example, in order to trace back and identify its ultimate beneficial owner.

Identifiers of media are not a new idea per se. Most, if not all, major stakeholders concerned (such as social media platforms and search engines, the advertising sector and public actors, such as national regulators, and academic researchers) already use their own identifiers to index media companies, their outlets, brands and channels, but those lists are often incomplete and not harmonized. The UMId is an effective and transparent alternative or complement to these diffuse attempts, which will mitigate related risks by facilitating harmonization – both vertically (between platforms and signal providers) as well as horizontally (platforms, ad-tech amongst each other respectively) – thus reducing errors, speeding up the processes, as well as preventing mismatches and mix-ups that are common in this space.

Many countries and transnational entities are currently in the process of updating their regulatory frameworks to better reflect the realities of the online environment, safeguard transparency and protect the rights of users. Assigning news sources with UMIDs would enable key players to more effectively comply with this kind of regulation. Some examples from the EU context are the Digital Services Act that requires online services to take effective mitigation measures against online risks, and the Copyright Directive which obliges online platforms to pay rights holders for their content. The European Media Freedom Act foresees a protected status for news media publishers and their accounts on social media, and the co-regulatory Code of Practice on Disinformation prescribes indicators of trustworthiness of online sources, to better inform users, guide content recommendation and to make advertising placement more transparent. At the same time, the assigning and managing of the UMId needs to comply with the General Data Protection Regulation, and some other laws inside and outside the EU.

As highlighted above, current efforts to assign identifiers to online media have some shortcomings. A problem occurs when different lists categorise accounts according to different criteria. This might be the case with brands of the same name (there are several dozens of media outlets called ‘Phoenix’), or with affiliates, syndicated channels or sister-brands of the same origin, that might follow different editorial lines (e. g. Al Jazeera, Phoenix or Fox). Even when a web-domain or social media account is always distinct, it might not be immediately clear to which media outlet or company it belongs. This could lead to conflicting or wrong signals, misleading algorithmic indexation and negatively impacting site integrity and user experience. Bad actors could even capitalise on this deficiency and try to game the recommender systems with similar sounding names of channels, accounts, or brands.

The instrument of industry standard setting is a useful path to solve the outlined problem in a fully self-regulatory and consensual, but still authoritative way. Examples of such conventions are the two-

or three-letter country codes stipulated by ISO, the three letter codes for airports, or the international bank account number (IBAN). Specific to the content creation process, the International standard name identifier (ISNI) is an identifier for the public identity of parties.

The UMId project has been proposed by the Global Media Registry, a Germany-based non-profit social enterprise that supports transparency, accountability, and pluralism in the digital information space. The GMR is a member of the Global Forum for Media Development (GFMD), a consortium member of the Global Media and Internet Concentration Project (GMICP) and a member of the Media Freedom Cohort of the Summit for Democracy. The proposer of the workshop has, in advance, taken into account the work of existing ISO/TCs such as:

- ISO/TC 46/SC 9 Identification and description
- ISO/TC 204 Intelligent transport systems
- ISO/TC 289 Brand evaluation
- IEC/TC 100 Audio, video and multimedia systems and equipment
- ISO/IEC JTC 1 Information technology

Members or officials of the above-mentioned ISO/TCs have actively participated in the elaboration of this IWA. The IWA 44 workshop members have organized themselves in dedicated subgroups on certain aspects (clauses) of this document:

- Subgroup on Syntax and taxonomy to identify a possible format and the elements that are most suitable for the UMId, based on use cases. This work includes the definitions of terminology, the entity relationships, and the scope of applicability, for example with regards to individuals;
- Subgroup on Operations and governance to identify the aspects relevant for assigning and managing the UMId, including recommendations for possible entities involved in the process and their roles in the governance, possible methods of assigning UMId keys (e.g. automated, curated or mixed) and business model considerations;
- Subgroup on integrity, transparency and security to assess relevant aspects of security, to identify mechanisms to prevent misuse and to ensure that the UMId could serve as a trusted resource for the industry and audiences.

IWA 44 - Unique Media Identifier (UMId) for distribution channels and brands

1 Scope

This document provides requirements and recommendations for the structure, associated metadata to be included and the governance of the Unique Media Identifier (UMId) that can be assigned to all media outlets that publish content online. The identification of material or physical objects is out of scope of this document.

The aim of the UMId is to establish source identity, including a clear connection between channels operated by the same editorial unit across platforms, including news media websites and their social media presence. Such an interoperable system of UMIDs is crucial to safeguarding the integrity of news and information ecosystems, which is relevant when publishing, accessing, and managing content online.

Additional parties engaged in this information ecosystem such as individuals (influencers, bloggers, or independent journalists), as well as third-party aggregators and other distributors may be considered for UMId assignment.

Unique Media Identifiers (UMId) are one of the possibly multiple components of an open and scalable infrastructure of identifier systems and indicators that aim at safeguarding the transparency, responsibility and accountability of online content and its sources. The purpose of this proposal is therefore not to replace existing standards and indicators, but to add a holistic and global framework with a view on harmonising them.

The IWA also considers the UMId's technical infrastructure and its practical implementation.

This document is a neutral, non-judgemental numbering or naming convention, not a certification scheme. Thus, it does not include any requirements for the assessment of online content – for example as regards its "trustworthiness" or quality – or an outlet's compliance with journalistic standards.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 639-2, *Codes for the Representation of Names of Languages*

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions*

ISO 17442 (all parts), *Financial services — Legal entity identifier (LEI)*

ISO/IEC 7064, *Information technology — Security techniques — Check character systems*

ISO/IEC 10646, *Universal coded character set (UCS)*

IETF 4648, The Base16, Base32, and Base64 Data Encodings

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1

UMId system

technical and management infrastructure that supports the assignment of UMId keys (3.2) and provides for the network's long-term maintenance, resolution and governance

3.2

UMId key

alphanumeric string representing a unique outlet (3.10) in the UMId system

3.3

code point

value in the Universal coded character set (UCS) codespace

[SOURCE: ISO/IEC 10646; 3.9]

3.4

UMId syntax

rules for the form and sequence of code points (3.3) comprising any UMId key (3.2), specifically the form and sequence of code points of a UMId prefix element (3.5) and suffix element (3.6)

3.5

UMId prefix

unique string of code points (3.3) forming part of the beginning element of the UMId syntax (3.4)

3.6

UMId suffix

unique string of code points (3.3) forming part of the ending element of the UMId syntax (3.4)

3.7

kernel UMId metadata

specific data associated with the outlet (3.10) identified with a UMId key (3.2), that is based on a data model that is sufficient to uniquely identify the Outlet

Note 1 to entry: kernel metadata is specified in Annex A;

Note 2 to entry: kernel metadata is mandatory in the metadata model.

3.8

extended UMId metadata

specific data associated with the outlet (3.10) identified with a UMId key (3.2), that provides additional information related to outlet

Note 1 to entry: examples of extended metadata are specified as optional in Annex A;

Note 2 to entry: extended UMId metadata is managed by the Issuing agent (3.9) with data of any desired degree of precision and granularity to support identification and description in their market (3.12).

3.9

Issuing agent

organization that assigns and registers a particular UMId key (3.2) to an outlet (3.10)

Note 1 to entry: Issuing Agents are registered and accredited within the UMId system (3.1) by the UMId Registration Authority.

3.10

media outlet

editorial entity that is the source of content with designated staff, distribution channels (3.14), assets (3.15) – i. e. content brands (such as publications, shows, etc.) and frequent/periodical output.

Note 1 to entry: There is at least one ultimate beneficial owner (3.12);

Note 2 to entry: Usually, a legal entity (3.11) is affiliated with the outlet;

Note 3 to entry: Different channels of one outlet can target different media markets (3.13).

3.11

legal entity

a registered body, usually a company, which is formed and owned by one or more natural persons to engage in commercial activities

Note 1 to entry: Through its registration it is always tied distinctively to one country but might operate in several language markets (3.13).

3.12

owner

a natural person who owns or controls a legal entity (3.11), typically through shares and voting rights as its (ultimate) beneficiary

Note 1 to entry: A special case is the State as an owner, mostly represented by public law bodies, like a ministry or other authority instead of natural persons.

3.13

media market

target area of outlet (3.10) as a combination of the geographical or territorial dimension, defined by at least one country or more, and one language or more

Note 1 to entry: Target MARKETs can differ from jurisdiction (country) where an outlet (3.10) is registered and/or operates from.

3.14

channel

distribution channel of a media outlet (3.10) and its editorial content

Note 1 to entry: For example, an FM radio frequency, a social media account or streaming channel;

Note 2 to entry: A channel is always distinct and tied to one outlet;

Note 3 to entry: The affiliation of a channel might be ambiguous or fully covert (e. g. anonymous social media accounts, impersonation, 'pirate' radio stations);

Note 4 to entry: Different channels (3.13) of one outlet (3.10) can target different markets (3.13).

3.15

asset

a content brand, like a show, segment or publication title under a media outlet (3.10)

4 Construction of a UMId

4.1 General characteristics

A UMId key shall consist of an ordered sequence of case-insensitive alphanumeric code points encoded URI-safe base64uri character set as defined in IETF RFC 4648 using the alphanumeric Latin characters A-Z in capital and lowercase and the numbers 0-9.

Note: The term code point is used instead of the term character, which is ambiguous in the context of Unicode where a given abstract character can be encoded in multiple ways.

The code points are arranged in a UMId prefix and a UMId suffix and a two-element check digit.

1. UMId prefix

   A UMId prefix shall consist of a string of four code points and shall be assigned by the UMId Registration Authority to the issuing agent.

2. UMId suffix

   A UMId suffix shall consist of a string of sixteen code points, with fourteen code points identifying the outlet and the final two code points being a checksum. The UMId suffix shall be assigned by the UMId issuing agent.

Table 1 shows the structure of the UMId key.

Table 1 — Example of a UMId Key

UMId Code Point	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	UMId prefix: Issuing Agent Code – Assigned by the Registration Authority				UMId suffix: Identifier for Outlet – Assigned by the Issuing Agent										UMId checksum digits	
Example	Z	Z	Z	Z	X	X	X	X	X	X	X	X	X	X	#	#

The last two characters of the UMId suffix shall consist of a check digit element to ensure the validity of the UMId Key. The method for calculating the check digit element is described in clause 5.

Further constraints on code points (e.g. the use of numeric characters only) can be defined for an application by either the UMId Registration Authority or by the issuing agency.

The combination of a UMId prefix (assigned by the UMId Registration Authority to a particular UMId issuing agent) and a UMId suffix (assigned by the issuing agent to a specific outlet) shall be unique. While UMId prefix may be duplicative within the context of a specific issuing agent, and alternatively a UMId suffix may be duplicated across different issuing agents, the combination across the issuing agencies name spaces should prevent UMId conflicts. This allows the decentralised allocation of UMId keys. The registration of the combination of the prefix and suffix in the UMId system serves to validate the UMId syntax for a given UMId key. Care should be taken to ensure that the same outlet is not identified multiple times through the use of a deduplication process before the assignment is registered.

In a human-readable context, the UMId key should be displayed as “UMId: ” followed by the UMId key. For human readability, the UMId key may be separated by spaces but these spaces are not to be considered part of the canonical representation of the UMID key.

For interoperability purposes with other identifiers (such as DOI) or for human readability the UMId prefix and UMId suffix may be separated by U+002F SOLIDUS. The canonical UMId key shall be the code point string without the solidus separator.

Note: U+002F SOLIDUS is also referred to as forward slash ("/").

The UMId key shall be regarded as an opaque string by users of the UMId system. No definitive information shall be inferred from the specific sequence of code points that make up a UMId key. In particular, the inclusion in a UMId key of any UMId prefix allocated to a specific issuing agent does not provide evidence of the ownership of rights, the current management responsibility of any intellectual property in the referent, or in any relations to the geographical location of the owner of the outlet. The mere assignment of a UMId key shall not imply endorsement of the outlet by any party.

5 UMId Check Digit

5.1 General characteristics

The UMId suffix shall end in a two-code point check digit unit. This unit shall be calculated and appended to the first 18 code points of the UMId key, including both the prefix and the first fourteen code points of the UMId suffix. The check digit pair is used to verify that the UMId key is properly formed.

The check digit pair shall be calculated based on the simplified procedure defined in ISO/IEC 7064 (MOD 97-10) after the conversion of the leftmost 18 alphanumeric characters of the UMId key consisting of both the UMId prefix and the UMId suffix into a character string consisting only of digits.

Valid check digit pairs are in the range of [02 .. 98]. 00, 01, and 99 are not valid UMId check digit pairs.

If the check digit pair has been calculated correctly, when the entire 20-character UMId is converted to numbers following the process described in 5.2 step 1, and divided by 97 as described in 5.2, step 3, the reminder shall be "1".

5.2 Procedure for calculating the check digit unit

Step 1: The value of any code points that represent digits shall be equal to their numeric digit value between 0 and 9. Any code points representing letters in the first 18 code points of the UMId key shall be converted to digit pairs in accordance with the table described below.

A (or a) = 10	F (or f) =15	K (or k) =20	P (or p) =25	U (or u) =30
B (or b) =11	G (or g) =16	L (or l) =21	Q (or q) =26	V (or v) =31
C (or c) =12	H (or h) =17	M (or m) =22	R (or r) =27	W (or w) =32
D (or d) =13	I (or i) =18	N (or n) =23	S (or s) =28	X (or x) =33
E (or e) =14	J (or j) =19	O (or o) =24	T (or t) =29	Y (or y) =34 Z (or z) =35

Step 2: Two zeros shall be appended to the resulting string at the rightmost positions.

Step 3: A Euclidian division of the resulting number by 97 shall be performed to determine the remainder.

Step 4: The remainder shall be subtracted from 98 to determine the check digit pair.

Step 5: The check digit pair shall be appended to the original 14 alphanumeric characters to form the 16-charachter alphanumeric string.

5.3 EXAMPLE

Examples of this model:

- **9523Gg2t87xz8H53** – 9523 (Issuing Agent) Gg2t87xz8H (identifier of Outlet) 53 (Checksum)
- **8802Uu877V2Mo770** – 8802 (Issuing Agent) Uu877V2Mo7 (identifier of Outlet) 70 (Checksum)

Note 1 to examples: These examples are fictional UMId keys and one should not infer an implementation model of the UMId key based on these examples;

Note 2 to examples: To avoid collisions with other related ID systems, which may be interoperable with the UMId system, the Registration Authority needs to work with other identification systems to set aside reserved code blocks in related namespaces where UMId and other identifiers may overlap to ensure that there is not duplicative assignment of identifier strings.

6 UMId kernel Metadata Elements

6.1 General characteristics

The UMId kernel metadata captures those attributes that are core to identifying and disambiguating the media outlet, as well as to ensure proper management of the UMId system. An issuing agent must generate a complete UMId kernel metadata record in the system for a resulting UMId key to be valid.

UMId kernel metadata are all required attributes of a UMId systems record. Some of these attributes may be withheld from public distribution of media outlets within the UMId system.

The UMId kernel metadata must include the following attributes:

— the UMId key

— the name of outlet (could include transliterations as a data array)

— the owner of the outlet (could be represented by an organizational identifier, such as LEI)

Note to owner: Owners may be anonymous, or unknown to the issuing agent.

— the language(s) of the outlet (as represented using ISO 639)

— Media market of the outlet (could be an array of geography and language)

— the country / jurisdiction of the outlet (represented using ISO 3166 codes)

Note 1 to country: Some regions may not be formally recognized and therefore not have an official ISO 3166 Code assigned. In these cases, this field should be populated using Specially Reserved Codes as defined in ISO 3166-1 to identify geographic regions which the origin is clear but where a country is not formally recognized;

Note 2 to country: If the country of origin is unknown, the country of assignment will be noted, with the notation "(assigned in)" to avoid confusion with the location of the origin.

— the date of assignment

— the date of last amendment to record

— the media type or types, if there are multiple, of the outlet (i.e., print, digital, broadcast TV, radio, etc.).

Full details of the UMId kernel Metadata elements are specified in Annex A.

The Registration Authority may establish additional required fields beyond those described here in the implementation of the UMId system.

7 UMId Extended Metadata Elements

7.1 General characteristics

The UMId metadata record may contain other metadata elements that provide additional context and information regarding the outlet, its owners, markets, or other attributes worthy of the investment of creating and maintaining the information. This extended metadata record is managed by the issuing agent. Some of these data may be shared with the Registration Authority.

Additional metadata which are desirable, although not mandatory are specified in Annex A.

The Registration Authority or issuing agents may establish additional metadata elements beyond those described here in the implementation of the UMId system.

8 UMId Assignment

8.1 General characteristics

The UMId shall not be construed to replace other identifiers, such as ISSN, ISAN, ISNI, LEI, and other commonly recognised identifiers.

Rules for assignment of UMId keys and UMId extended metadata can vary based on a functional definition of the assignment scope based on the requirements of an issuing agent.

The UMId key shall be associated with kernel metadata that describes the referent to which the UMId name is assigned.

Specific attributes of kernel metadata may not be available in some circumstances. Terms like "unavailable" or "anonymous" might be included in attributes and metadata associated with a UMId that have been withheld.

9 UMId Interoperability with other IDs

9.1 Interoperability with DOI

The UMId key allows for the use of the code point U+002F (i.e., solidus or forward slash) as an alternate representation of UMId key string. This allows for the capability for interoperability of the

UMId with the DOI system as defined in ISO 26324 and the DOI Registration Authority. In the use case where the UMId is integrating with the DOI system, the UMId prefix shall be represented with the DOI prefix and the UMId suffix shall represent the DOI suffix, with the two separated by the U+002F code point. Further integration between the metadata schema for UMId and the DOI shall be addressed in coordination between the UMId Registration Authority and/or a UMId issuing agent and the DOI Registration Authority.

9.2 Interoperability with QR Codes

The UMId key is defined as being case-insensitive using base64uri characters. It is noted that the encoding of lower-case characters in a QR Code requires significantly more data representation in the code processing, as described in ISO/IEC 18004:2015 Information – Automatic identification and data capture techniques – QR Code barcode symbology specification. Therefore, it is recommended that in the use case of a UMID being applied to a QR code the UMId should be represented as being in capital letters to improve interoperability with the QR code standard.

Annex A
(normative)

Metadata elements

A.1 Metadata elements

Table A.1 shows the metadata elements associated with a UMId key.

Note 1 to Table A.1: Some of these data elements may be arrays of information in an operational system, to record history, changes, valid keys, or other data that may change over time;

Note 2 to Table A.1: Some of these data elements may be unavailable, anonymous, or withheld in various circumstances. The Registration Authority may establish rules for how issuing agents handle data.

Table A.1 — Metadata Elements

Kernel/required – or – extended/optional	Element	Description	Related information
REQUIRED	UMID KEY	The UMID KEY code point string	
REQUIRED	NAME OF MEDIA OUTLET	Identified Source Name, in original LANGUAGE/script	
REQUIRED	LEGAL ENTITY	LEGAL ENTITY that operates the OUTLET	LEI (or alternate if noted)
OPTIONAL	LEGAL ENTITY TYPE	Controlled vocabulary of OWNER types, such as government, corporate, non-profit.	
REQUIRED	ULTIMATE BENEFICIAL OWNER	Natural person or public law body that owns and controls LEGAL ENTITY.	
OPTIONAL	VARIANT NAMES	Variant names of the OUTLET/Publication (acronyms, etc.), repository of brand names including logos.	
OPTIONAL	CHANNELS	Structured repository of distribution channels of OUTLET	
OPTIONAL	ASSET	Content brand, like a show, segment or publication title under a media OUTLET.	
REQUIRED	MARKET	Geographical/territorial area that the OUTLET targets, defined by one or more COUNTRY.	ISO 3166

Kernel/required – or – extended/optional	Element	Description	Related information
REQUIRED	LANGUAGE	Primary language of the content in the OUTLET	ISO 639
REQUIRED	COUNTRY	Jurisdiction in which LEGAL ENTITY is registered	ISO 3166
REQUIRED	INTERNET DOMAIN	Internet domain of the OUTLET	DNS URL
REQUIRED	DATE	Date of Assignment/Record update	
REQUIRED	CATEGORY	Category of OUTLET	Controlled vocabulary of the category of the Outlet, such as print, web, audio, video, etc
OPTIONAL	RELATED ENTITIES/IDENTIFIERS	Identifiers of related entities (owners, translations, republishers)	If not directly related to Channel or Outlet from above
OPTIONAL	RELATED IDENTIFIER TYPE	Description of the identifier type	More information about the Related IDs above
REQUIRED	REGISTRANT	Entity that requests the identifier	
REQUIRED	PLACE	Location of the OWNER (Could be as specific as an address, or as general as “City/Country”)	
REQUIRED	ISSUING AGENT	Entity that recorded the registration	Administrative metadata
REQUIRED	VERIFICATION STATUS	Corroboration level of data	Controlled vocabulary determined by the Registration Authority
REQUIRED	REGISTRATION STATUS	Status of the OUTLET, such as “Active”, “Ceased”, “Inactive”, etc.	Administrative metadata
REQUIRED	REGISTRATION STATUS DATE CHANGE	Date of last status change	Administrative metadata
OPTIONAL	REGISTRATION CONTACT	Contact information of the registering entity	Administrative metadata

Kernel/required – or – extended/optional	Element	Description	Related information
OPTIONAL	PUBLIC SIGNING KEY	Used for cryptographic id	

354

355 **Table A.2 — Fictitious Examples of Metadata Set**
356

Kernel/required – or – extended/optional	Element	*fictitious example #1*	*fictitious example #2*
REQUIRED	UMId Key	9523Gg2t87xz8H53	8802Uu877V2Mo770
REQUIRED	Name of Media Outlet	The Springfield Daily Online News	TV1
REQUIRED	Legal entity	Daily News Foundation (LEI: 94AAF735A7170011FA84)	First Channel Media Ltd. (LEI: 493001KJTIIGC8Y1M12)
OPTIONAL	Legal Entity TYPE	non-profit	corporate
REQUIRED	Ultimate beneficial OWNER	N/A (member owned)	Jane Doe
OPTIONAL	Variant Names	SDON, The Springfield Daily, SpringDay	Channel 1, The First, TV1
OPTIONAL	Channels	www.thespringfielddaily.co.uk (open-web), @springfield-daily (YouTube; streaming platform), @springfield-news-online (X, Facebook, Instagram, Snapchat; social media platforms)	www.firstchannel.xx (open-web), @firstchannel, @tv1news (YouTube; streaming platform), @1stchannel (X, Facebook; social media platforms), 2.0° E 1115 MHz H (Star satellite), UHF channel 45, 656 MHz (terrestrial broadcasting)
OPTIONAL	Asset	SDON-Kids, SDON local newsletter, Springfield4You, City-Council LIVE	Daily News Hour, Quiztime, Morning Show, etc.
REQUIRED	MARKET	GBR	[XXX]
REQUIRED	Language	eng	eng

Kernel/required – or – extended/optional	**Element**	***fictitious example #1***	***fictitious example #2***
REQUIRED	COUNTRY	GBR	[Country X]
REQUIRED	Internet Domain	www.thespringfielddaily.co.uk	www.firstchannel.xx
REQUIRED	Date	07/08/2024	24/03/2024
REQUIRED	CATEGORY	web	audiovisual broadcaster and web
OPTIONAL	Related Entities and Identifiers	N/A	Movie Channel Y
OPTIONAL	Related Identifier Type	N/A	UMID Movie Channel Y: WvbtU59zAJHYeo33
REQUIRED	Registrant	Daily News Foundation	Media Empire Holding Inc.
REQUIRED	Place	Springfield, United Kingdom	Exampletown, [Country X]
REQUIRED	Issuing Agent	IMPRESS	ID-Hub Ltd.
REQUIRED	Verification Status	verified	verified
REQUIRED	Registration Status	active	active
REQUIRED	Registration Status Date Change	07/08/2024	09/09/2024
Optional	Registration Contact	16-18 New Bridge Street, London, England, EC4V 6AG	123 Streetname, Othercity, [Country X]
Optional	Public Signing Key	N/A	MCowBQYDK2VwAyEA4oxcRUfK5BuwXI5dF4D2p0/fEgRkMYPxYbghx2uwYXM=

357

Annex B
(informative)

Governing and Operating the UMId

B.1 General

B.1.1 Purpose

The success of the identifier will depend on demand for it and this can only be met and further nurtured if suitable governance and operational structures are in place to issue the identifier and to maintain it together with its related reference (meta) data.

The purpose of this annex is to lay out requirements for such an infrastructure, including recommendations of how to implement it.

It was decided to choose the format of a reference document, annexed to the actual workshop agreement, in order to emphasise the difference in character of these two main chapters. While the specification of the actual identifier, as constituting the main body of this workshop agreement, might be further developed into an ISO standard later on, the requirements and recommendations regarding governance and operational models could in parts, but do not necessarily have to be included into that trajectory of codification.

B.1.2 Guiding principles and references

The path of a workshop agreement was chosen by the proposer as a suitable instrument to produce a result swiftly, meeting the urgent demand expressed by a variety of stakeholders. With this in mind, the implementation is also expected to unfold and make the identifier available for usage as quickly as possible.

Secondly, efficiency was mentioned throughout the development process as a main principle to adhere to. In practical terms this means to build, preferably, on existing knowledge and structures, rather than creating redundancies.

Thirdly, the integrity of the overall endeavour is considered key. This principle is a given for any identifier to function and thrive, but perhaps even more important in the context of media and information. Different from many other industries, potential risks of fraud or infringements might not be motivated by financial gains only but could also be driven by political or ideological purposes.

This document has been informed by ISO/TS 22943: Information and documentation – Principles of identification, as a main benchmark.

Other relevant sources are listed in the bibliography.

B.1.3 Centralized vs. decentralized model

Governing and operating an identifier like UMId at a global scale requires significant resources and structures in place. Both a centralized and decentralized model might be considered to achieve this goal, with each of them having distinct advantages and disadvantages.

From a practical perspective, a centralized structure would require significant investments that are not considered feasible, let alone matching the general principles of speed and efficiency. Insofar, also with a view on capitalising on existing structures and actors in the field of digital identity, a decentralized structure of implementation seems worthwhile to consider.

On the other hand, essential requirements related to the overall integrity, but also conflict escalation and mitigation, as well as external representation, would call for a certain hierarchy that might be better represented by a centralized structure.

In order to combine the advantages of both models, a hybrid solution is recommended according to which a decentralized, distributed or syndicated structure of operations (see pt. BIII. below) would be complemented by one lean, centralized governance body.

B.1.4 Economic considerations

The distinction between governance and operations also matters in terms of financing. While the former is generally designed to become a utility and not-for-profit public service, the latter might require a business model to scale through incentives, depending largely on the assignment tracks and types of actors involved.

Accordingly, the income foreseen to build and sustain the centralized governance structure is most likely a combination of public subsidies, grants and levies extracted from the operational level, possibly organized in a tiered model, depending on country context. There, different environments and use cases will determine the respective economic model. Given the expected worldwide, decentralized nature of the network for assignment, it is anticipated that the cost-recovery structure will vary by national origin and type of the assigning agency. They may range from the enforcement of regulation by public sector authorities, through investments into content moderation by commercial intermediaries, to a diverse ecosystem of assigning agencies to serve voluntary applicants.

While the economic concept is bound to be restricted to cost-recovery, rather than profit driven, actors may be encouraged to build and sell ancillary services as an additional incentive to consider becoming an assigning entity.

The concept of cost-recovery may also include the maintenance of an operating surplus to facilitate, for example, strategic and developmental plans associated with providing the Services.

B.2 Centralized Level of Governance

B.2.1 General

A centralized structure is considered essential to govern the overall UMId system. It is the guardian of certain core principles and responsible for enforcing them throughout a decentralized network.

Certain operational duties might also be located at the centralized level, for example for the purpose of efficiency or to safeguard coherence, while other duties and operational responsibilities might be situated at the issuing agency level.

B.2.2 Principles for a governance structure

ISO will appoint a Registration Authority (RA) to manage the UMId system, following a public call for applications. The principles below might be applied as criteria in the respective selection process, but also serve as a guideline to operate the RA further on.

a. Transparency, participation and representation

The strength of this identifier, its breadth of potential use cases, also brings about elevated requirements to cater to the needs of different stakeholders and represent them accordingly. This also means to balance potentially divergent interests to avoid any undue or disproportionate influence.

Transparency as a requirement of the governance structure is not considered an end in itself, but an essential prerequisite to sustain and further build the legitimacy of this identifier.

b. Interoperability and openness to change

Preliminary research during the proposal process and the subsequent development phase of this identifier has demonstrated the existence of a variety of relevant, neighbouring initiatives. While the specification of this identifier and its underlying logic are being built on them in a complementary manner, this ecosystem will remain dynamic and thus the need to constantly

cross-fertilize remains. This requirement is not only catering to the principle of ISO to avoid overlaps, but also meant to drive efficiency through interoperability.

It must be stated that the realm of digital policy and regulation is still in its infancy, thus developing relatively quickly and at different speeds around the world. Further propelled through technological breakthroughs, such as AI, the legislative environment is expected to remain dynamic and thus require the governance of this identifier to be agile, innovative and open to change.

c. Efficiency, effectiveness, ethical conduct and accountability

A proposed governance model needs to be realistic and fit for purpose. This includes the resources, capacity and skills needed to discharge its mandate in a professional, efficient and ethical manner.

To that end, suitable protocols for internal and external accountability must be implemented.

d. Independence and human rights

In this sensitive field of information integrity, it is of utmost importance to insulate the UMId system from any undue influence, including, but not limited to political pressure. To defend its independence and a human-rights-based approach, appropriate measures could include appointment procedures of directors, due impartiality provisions and suitable oversight structures.

e. Security

The integrity and legitimacy of this identifier depends on the overall, operational security of the system, of which the governance body is expected to become the supreme guardian (see Annex C).

B.2.3 Specific roles and responsibilities

a. Safeguarding the overall, internal integrity of the UMId

A decentralized model of operations requires a robust protocol to ensure the identifier's integrity. This includes the development and implementation of rules and protocols across the whole system, e. g. unified terms for assigning entities and appropriate measures to prevent duplicates from being issued.

In addition, systemic risk assessment and mitigation, including respective trust and safety protocols, is a responsibility of the UMId governance structure.

b. Facilitating operations

With a clear distinction between centralized governance and decentralized operations, it is important to define the interface between these two layers. This manifests in the role a governance structure can and must play to facilitate operations.

One of those central roles will be the appointment of issuing agencies, including suitable audit and compliance protocols (see below). Secondly, coordination between the three proposed assignment tracks can only happen at a 'higher' level. This also includes transition rules between these different tracks.

In addition, coordinating the physical storage and provision of data, including catalogues, interfaces and other protocols and means of accessing, securing, and exchanging them, is an operational task located at the centralized level.

Furthermore, the centralized level's tasks include providing documentation for users and issuing agents, as well as collating and analysing statistics on operations.

c. Securing external interoperability and consistency

In addition to safeguarding the internal integrity of this system (see above), continuous monitoring of and potential harmonisation with relevant neighbouring standards is essential. This would involve both existing and new initiatives in this space. Interoperability is a key feature of this identifier and thus, proactive exchange at the technical and also the policy level is considered key.

This quest also covers the regulatory environment, where a requirement for the governance structure is to monitor and assess developments on a rolling basis.

d. Providing accountability and compliance throughout the system

A central structure, also in a hierarchical sense, is necessary to escalate and resolve potential conflicts within the system. This would, for example, include complaints and alternative dispute resolution (ADR) mechanisms, frequent audits and independent review processes, advisory and oversight boards.

e. Representing the UMId

Within the ISO system, but also vis-à-vis other external stakeholders, the UMId needs a unified representation in order to communicate and, if needed, to defend its role. This would include the participation in relevant technical committees and bodies, as well as coordinating government and institutional relations, advocacy and PR across the network. Representation should also include activities focused on promotion, education and training.

f. Development (a learning system)

This identifier is located within a highly dynamic and fast-moving environment of technological progress. Use-cases and demand will develop accordingly, also defined by potential regulatory action in this space. Insofar, constant adjustment of the UMId logic and protocols is an essential requirement of all actors involved, with a centralized governance structure in charge to coordinate.

g. Financial self-sufficiency

The Registration Authority must define, implement and maintain such funding arrangements as are necessary to support its operations.

h. Risk mitigation

The overall risk assessment, on a rolling basis, as well as the oversight of effective risk mitigation protocols is a task of centralized governance bodies (see Annex C).

B.3 Decentralized Model of Operations

B.3.1 General

A decentralized network of entities is considered essential to scale operations of the UMId system, but also to ensure responsiveness to adapt to a variety of markets and use cases.

However, operational actors – such as issuing agencies – are not only subject to the overarching, centralized governance, but also actively contributing to it in return.

B.3.2 Features of an operational model

a. Scalability across markets and geographies

Assignment of, or easy access to, an identifier must be secured for all media outlets alike. This requires an operational strength to manage the amounts of potential cases (even more so at the beginning), but also to cater to the specificities of markets and the variety of actors.

This will become particularly important when political pressures might negatively impact the fair and equal assignment process in a certain place. In those cases, alternative avenues of assignment must be made available.

b. Sustainability

Based on a cost-recovery model, the operation of this identifier scheme requires investment into infrastructure, as well as a constant flow of revenues to sustain its implementation. Depending on the different tracks of assignment, different funding models will apply to incentivise actors to provide services in the space to begin with, and then provide a durable business model.

As it is the case with other successful identifiers, the possibility of inventing and offering ancillary, but non-mandatory for-profit services around the UMId assignment could become one such incentive.

c. Data coherence, exchange and availability

A federated system of assigning and maintaining identifiers brings about a requirement for all participating entities to contribute to the coherence of the whole system. This means to commit to general principles like independence and the respect for human rights, but also very practically to follow common rules and practices stipulated through the centralized governance model. More specifically, the interoperability of data, access and exchange both within the system and vis-à-vis external stakeholders must be secured.

Ensuring identifiers remain up-to-date requires constant monitoring and reviews, which are also a requirement for the operational model to deliver.

d. Flexibility according to different use-cases

One advantage of a decentralized system is its agility when it comes to adjusting to different environments and use-cases. This is an operational requirement that participating stakeholders have to live up to, also with a view on further developing the overall system.

e. Robustness against risks and threats

Part of the operational implementation is the ongoing assessment and, respectively, mitigation of internal and external risks. This requires the suitable protocols being in place and enforced throughout the network of participating entities (see Annex C).

f. Outreach

By their engagement with the system, participating entities become the public face of UMId in their respective marketplaces. It is in their own best interest to promote it proactively and thus, support its growth.

B.3.3 Assignment tracks

Broadly speaking, the assignment of identifiers follows two separate, but complementary logics – one is voluntary, the other is non-voluntary. In the latter category, media outlets do not have a choice, but will receive a UMId regardless. This could happen as an integral part of the statutory licensing process for broadcasting, or through membership in professional associations or self-regulatory mechanisms, like press councils, where the issuing of a UMId might become mandatory. Another possibility of the non-voluntary logic is to track and trace certain actors online, that are neither subject to regulation, nor members of like-minded bodies.

The first two assignment tracks below, a) and b), follow this non-voluntary logic and assignment entities might include institutional regulatory bodies, press councils or professional associations on the one hand ('Assigned and Certified'), or intermediaries enforcing their trust and safety policies in content moderation on the other ('Observed').

However, some media outlets do not fall into the non-voluntary category, but might still want to proactively seek and receive an identifier. This voluntary ('Self-reported') logic should be catered for, too, with a third assignment track c).

Before a UMId can be assigned under any of the assignment tracks detailed below, the issuing agency will be required to be accredited and appointed by the centralized governing body. The accreditation

process will involve the governing body assessing the applicant issuing agency's proposed operational, financial and technology processes and controls for issuing a UMId. The governing body may create simplified accreditation processes, but whether simplified or not, formal documents will need to be exchanged between the governing body and the issuing agency to confirm the terms of the appointment.

a. Assigned and Certified

This assignment track involves the information provided by applicant media outlets being verified and certified by an issuing agency as part of a non-voluntary process. For example, the issuing agency may be a professional body issuing a UMId as a condition of membership of their body, or a media regulator issuing a UMId if it has been integrated into a statutory licensing or authorisation process.

The issuing agency will review the information provided by the applicant media outlet against available information to determine whether it is satisfied to issue the identifier. For example, if the applicant media outlet is a registered corporate body, the issuing body may review this information against corporate entity registers in the relevant jurisdiction.

b. Observed

This assignment track is designed for media outlets that, for whatever reason, are not interested in receiving an identifier and do not fall under the assigned and certified track either. This might, for example, be the case for providers of content that appear anonymous, even actively disguise their identity, or imposters of legitimate brands.

It is expected that issuing agencies in this track might be intermediaries, such as distribution or social media networks, that enforce their respective trust and safety policies of content moderation, to enhance site integrity. This happens, more and more, also against the background of regulatory obligations and self-regulatory commitments.

One particular use-case is the coordination of rapid responses to mitigate harm of so-called 'bad-actors' that suddenly appear online across different platforms.

c. Self-reported

The rationale of this assignment track is twofold.

First of all, it should serve all media outlets that, for whatever reason, do not fall under the mandatory logic, but might still want to receive an identifier. This should, of course, be possible and facilitated through self-reporting and third-party validation.

Secondly, this track is meant to provide an alternative way of assigned and certified assignment for cases that, for whatever reason, are being left out.

Annex C
(informative)

Integrity, transparency and security of UMId

C.1 General

C.1.1 Purpose

The design, governance and operational structure of the UMId needs to ensure that systems, policies, procedures, and controls are in place to prevent misuse and to ensure that the UMId can serve as a trusted resource for the industry and audiences. Thus, risks and threats need to be addressed to prevent potential endangerment of entities identified or adversely affecting the reliable use of the UMId, for example by compromising data quality.

The purpose of this document is to provide a systematic overview of possible risks as well as recommendations of how to mitigate them in order to uphold integrity of the whole system, but also to implement the do-no-harm principle.

Risks can fall into two main categories: Risk that the UMId system might pose to others, and risk that the UMId system might be exposed to. The latter category subdivides into internal risk, coming from within the UMId network of stakeholders and contributors (internal risks) and risks coming from forces outside targeting the UMId system (external risks).

C.1.2 Transparency

The UMId contributes to a transparent media environment, and as such, the identification provided by the UMId, as well as the identity data collected as metadata during the different assignment procedures allow stakeholders to have a better understanding of media outlets, their owners and their asset structure. In order to provide meaningful transparency, the governance of the UMId system needs to ensure that data is widely accessible through databases of identified entities.

While transparency is key for the UMId system, the safety of those working for, running, or owning media (including digital safety and cybersecurity) is also a major concern. If full transparency of media-specific information might endanger individuals, the governing body and dedicated issuing agencies should provide alternative registration and vetting mechanisms for such media outlets and individuals, as well as allow for the storage and management of the data in a way that it can be kept confidential. At the same time, safety concerns shall not be misused to refrain from disclosure.

C.2 Risk categories and mapping

C.2.1 Risk exposure of UMId

A. External

External risks originate from actors outside of the UMId system over which its governance or management protocols have no control. These risks need to be anticipated, monitored and mitigated.

Such risks may include:

- Cyberattacks to compromise the UMId system in whole or in parts to render it dysfunctional, or hacking to tamper with data: External actors might have an interest to harm the initiative and do so by inflicting damage on its infrastructure or reputation;
- Unauthorised external access to protected data: actors that have an interest to disclose the identity and related metadata of vulnerable media outlets might try to compromise the respective measures to protect them;

- Undue political influence or regulatory pressure on UMId-related stakeholders: state actors might try to infringe the independence of the system to advance their goals;
- Technological advancements that impact the UMId design or procedures of implementation;
- General business and liability risks like fraud or blackmail, for example through ransomware attacks;
- Lack of demand and usage.

B. Internal

Internal risks occur within the purview and control of the UMId system and thus, are subject to effective compliance mechanisms to avoid or counter.

Such risks may include:

- Breaches of rules and terms of operations by individuals inside one participating entity or in the relationship between entities within the UMId system;
- Lack of data coherence or validity, for example through the issuing of duplicate identifiers or incomplete monitoring and updates;
- Malfunctioning of the system as such, including insufficient back-up and disaster recovery protocols.

C.2.2 UMId as a potential risk to others

Even if the UMId system is well protected against internal and external risks, it can result in unintended consequences, or even be actively misused against its intended purpose. Insofar, these 'outgoing' risks need to be considered in the design and implementation of this instrument as well.

- Certain ID holders might be at risk if protective measures are breached: the holding of an identifier, and the disclosure of identity-related data can put entities in physical danger, in cases when the data is not handled with sufficient caution or if the system is not sufficiently robust against unauthorised access;
- Potential of reputational, business and security risk of ID holders if data is wrong or outdated, be it due to internally or externally induced risk;
- Potential of reputational, business and security risk of ID holders if UMIds are captured, stolen or otherwise appropriated by third parties without authorisation, or sold by ID holders to third parties without notification;
- Inappropriate use of UMId by third-party actors (e.g. use of the identifier for undue, discriminatory measures, misuse as a trustworthiness indicator or even censorship) that might negatively impact single entities or whole ecosystems.

C.3 Threats and risk mitigation and measures (process approach)

C.3.1 Technical level: Design of the identifier

Identifiers need to be designed in a way that the use of the UMId is safe for the whole environment. This starts alre ady with the syntax, as an identifier that provides too much information in its string of characters can provide opportunities for misuse, thus, information included in the syntax needs to be kept at a minimum.

In addition, technological means of identification and protection, namely digital signatures with cryptographic keys, need to be considered to sovereignly signal affiliated channels of the holder of the identifier to be traced back to the original source, and to protect identity where necessary.

There also need to be sufficient safeguards already at the design level to prevent the misuse, misappropriation and altering of identifiers. For example, there should be reasonable measures in place to mitigate against unauthorised users appropriating, editing, or "hijacking" an existing ID.

As the UMId will rely on a rich metadata structure, this leads to additional considerations of integrity. In order to protect UMId holders and safeguard the integrity of the identifier system, thorough assessment needs to be made about the risk associated with the kinds of information collected (including the legality of collection and storing, as well as the costs and benefits associated with handling certain kinds of data) and adequate procedures and controls need to be in place to safeguard handling of data.

C.3.2 Distribution level: issuing the identifier

A robust vetting mechanism needs to be in place, and measures need to be taken to keep the data up to date. Quality of data can be checked by including in the metadata the time and mode of verification. Changes in metadata must generate a detailed historic record (audit trail) to document and validate those changes (who updated what, when and why). Media outlets operating in volatile environments, or for other reasons feeling threatened, should be given a chance to undergo a safe and secure procedure of data provision and vetting, and the possibility of pseudonymity.

C.3.3 Management and maintenance level

The operational structure needs to ensure that the system meets the highest standards in relation to data integrity and security, and access controls. Confidentiality of data needs to be provided, if necessary, even in the exchange process between governing body and issuing agencies.

A database needs to be available to all stakeholders of the process to avoid duplication of identifiers.

Interoperability also needs to be in the focus of risk mitigation measures. The UMId exists in an ecosystem of a variety of relevant, neighboring initiatives, which are complementary, and can be used to increase the efficiency and enrich the data structure of the UMId. In order to minimise the risks associated with openness in a dynamic, constantly evolving environment, it is important to take proactive measures and constantly monitor potential weaknesses.

C.3.4 Compliance level

A feedback loop and a reporting mechanism needs to exist between governance and the UMId-holders that enables swift solving of problems related to identification or downstream distribution (Issuing agency going 'rogue' as an example or misalignment between outlet and asset level). In addition, it has to be ensured that stakeholders making use of the UMId do so in line with the intended purpose of the UMId (acting as a value-neutral identifier for media outlets). Guidelines and terms of services should ensure that stakeholders abide by the principles of fairness.

C.3.5 Advocacy and educational level

Outside of the reach of the UMId system's governance, where terms of service and contracts would be applied to enforce rules and principles, additional efforts must be undertaken to encourage a wider community of stakeholders to use the identifier according to its intended purpose or to call out potential misuse. To that end, a code of conduct and recommendations for the ethical use of the identifiers should be actively promoted.

Annex D
(informative)

Guidelines and Best Practices for Potential Usage of the Unique Media Identifier (UMId) by External Parties

D.1 General

While most users of the UMId will be engaged in a contractual relationship with parts of the UMId system, such as the issuing agencies or recipients of the identifier, certain other third parties, for example state actors, online intermediaries, distributors or advertisers, can use and should use the UMId without becoming a part of the UMId system and thus, remaining outside of a contractually binding relationship.

As those users would not be legally subjected to complying with certain rules and obligations to implement the UMId, these guidelines lay out principles for the usage of UMId across the whole ecosystem to foster benefits, but also identify and mitigate misuse, be it intended or not.

D.2 Principles of usage

D.2.1 Nature

Users of the UMId should be mindful that the identifier is a neutral, non-judgemental numbering or naming convention, not a certification scheme that would serve to assess conformity with certain criteria. Thus, it does not provide information about the level or lack of trustworthiness or independence of a content provider, the accountability mechanisms in place, the editorial standards an outlet follows or the quality of the content it publishes.

D.2.2 Attribution

Users of the UMId should respect the purpose and strict neutrality of this standard and publicly reference the UMId when using it.

D.2.3 Transparency

The UMId is an identifier aiming at enhancing the integrity of the online news ecosystem.

Whoever uses it should do so in a transparent manner, by proactively and appropriately describing to all actors it might affect, especially the holders of the UMId and the general public, the ways they use the identifier and metadata associated with it.

D.2.4 Benefits and Sanctions

The UMId identifier itself should not be used as qualitative signal, for example to impose sanctions or penalties on media service providers – only because of the existence of absence of a UMId – or be used as an exclusive requirement to access certain services or benefits.

D.2.5 Unintended consequences

Third-party users of the UMId should constantly monitor the impact of the actions taken reliant on the UMId. If unintended consequences occur, corrections should follow. In those cases, users are also encouraged to share these experiences with the wider community to contribute to the healthiness of the overall UMId system.

D.2.6 Complaints

Third-party users should have appropriate mechanisms in place to handle complaints from UMId holders or other parties of the UMId system.

Annex E
(informative)

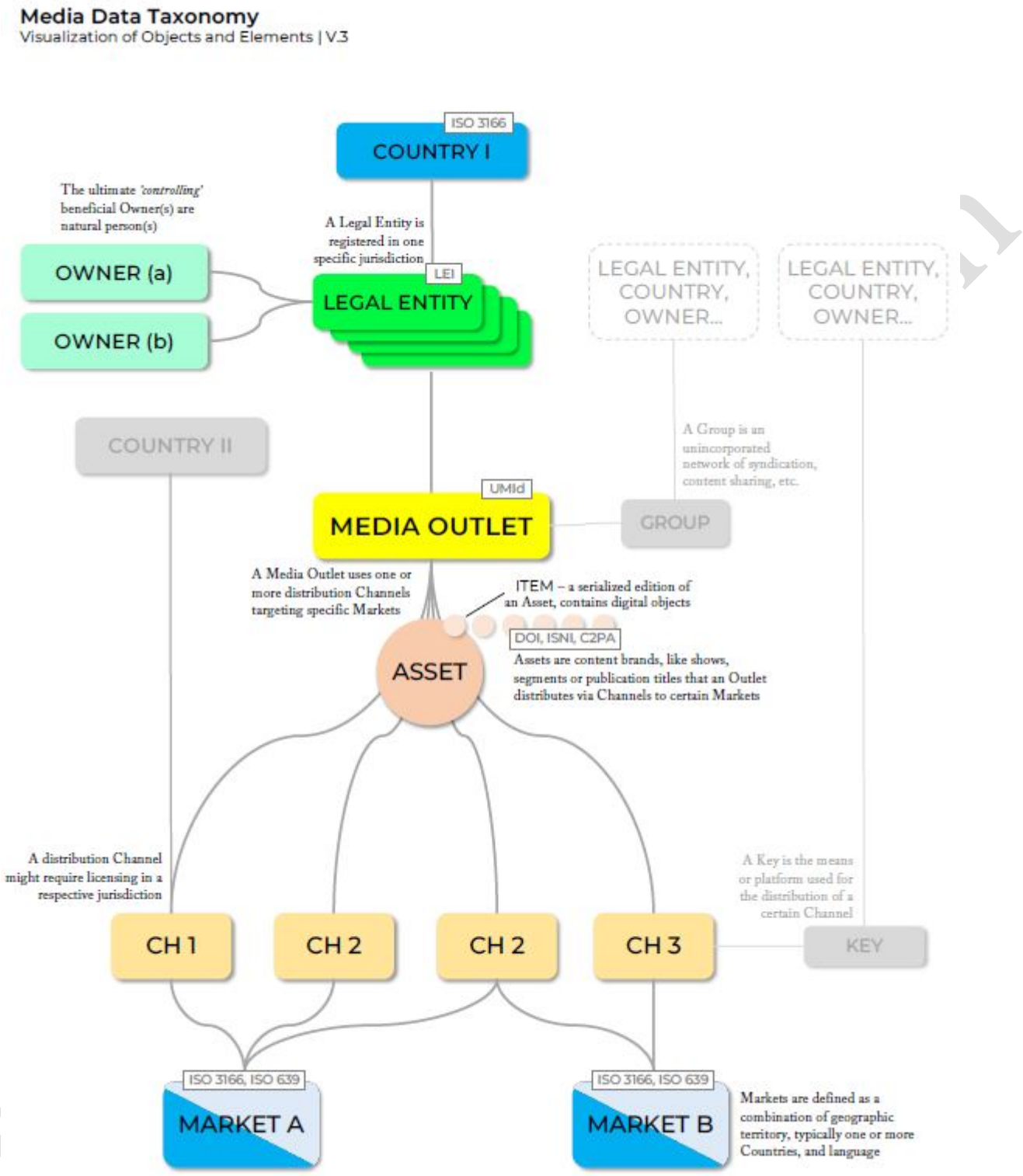
Media Data Taxonomy

E.1 General

The UMId system is designed to crosspollinate with neighbouring, existing identifiers, and provide a data-model that can be applied for a variety of use cases. The purpose of this Annex is to visualize the connectivity of the different metadata elements attached to the UMId, as well as adjacent identifiers.

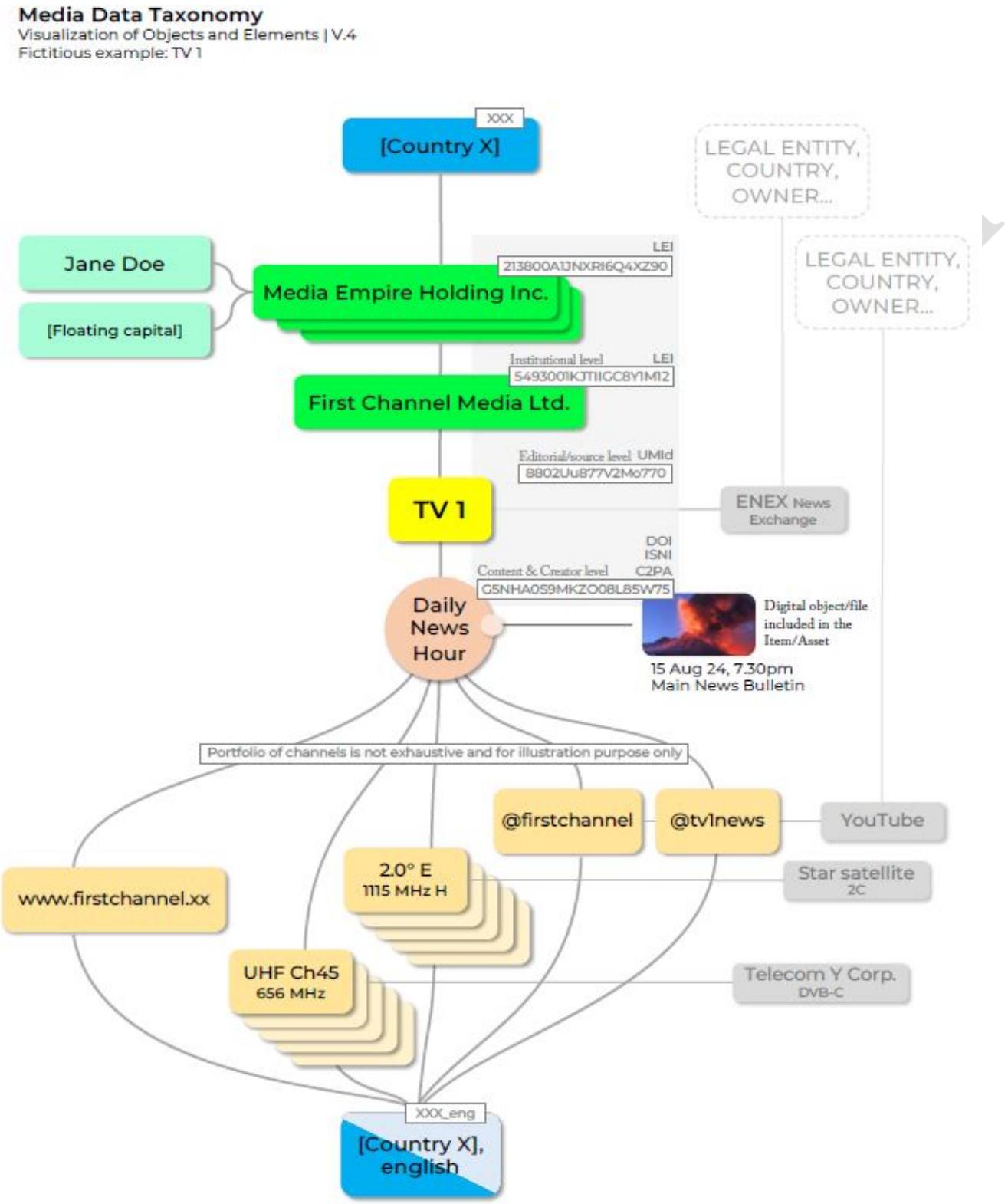
Figure E.1 visualizes the Media Data Taxonomy, based on the Metadata Elements defined in Annex A.

Figure E.2 visualizes the fictitious example #2 of Table A.2 based on the above.



786

787 **Figure E.1 – Media Data Taxonomy**



788

789 **Figure E.2 – Visualization of fictitious example #2**

Annex F
(informative)

Workshop contributors

Country	Representation	Name

Bibliography

[1] ISO #####-#, *General title — Part #: Title of part*

[2] ISO #####-##:20##, *General title — Part ##: Title of part*

https://www.coe.int/en/web/good-governance/12-principles#{%2225565951%22:[10

https://www.icann.org/resources/pages/mechanisms-2014-03-20-en

https://www.icann.org/resources/pages/governance/guidelines-en

https://www.gleif.org/en/about/governance/regulatory-oversight-committee-roc