Authentication and ensuring the freedom to operate

In today's knowledge-driven, hyper-connected world, creativity and intellectual assets – notably intellectual property – are critical success factors for many companies and individuals alike.

The value of such assets arises not only from their creation and the ability to create but also the ability to:

1. Prove the existence of content at a specific time
2. Protect integrity
3. Help ensure the freedom to operate and continue creating.

Prove the existence of your content and your creation at a specific time: Conclusively establishing that you created a piece of intellectual property – whether an invention, book, song, image, film, painting or software – at a specific date and time can mean that you get the recognition, and reward for your work.

Protect integrity: Being able to demonstrate that the item in question is genuine and not altered is not only useful to prove authenticity but also for ensuring the probative value of the item should it be used in subsequent legal action. Such authentication of integrity is vital in proving, for example, that records provided for regulators or photographs and other records created during forensics or other investigations were not tampered with.

Increased freedom to operate and continue creating: The IKR can help you to prove that you created and/or used a piece of intellectual property before someone else establishing a prior user right that, in some jurisdictions, may allow you to, for example, continue using that intellectual property increasing your freedom to operate against someone else who subsequently registered that intellectual property for himself then later attempts to use those rights to hamper your ability to work, to create, use, produce or sell that intellectual property.

Authentication in the past
In the past, one might have attempted to document the creation – or the process of creating something new – through the use of photographs with film-based cameras, written notes, or even images using chemical-based media. The use of these same techniques is both costly and impractical in today's world.

Enter the IKR (International Knowledge Registry)
Today you can take advantage of digital technology to create new intellectual property or document the creation of new intellectual property – then obtain an IKR record for:

- Each new file created
- Each picture taken of the work or art in creation
- Each copy of the new software being created
- Each new version of a document made, or even
- The log entry noting an important breakthrough for the creation of a new invention.

IIPCC's Certification process, the IKR System, enhances the value of intellectual assets by creating a unique identifier (an IKR record) for each asset – or version of the asset.

By also recording both the date and time of the creation of the work[1] the IKR record authenticates the existence of the contents of the digital asset at a specific date and time.

The IKR record along its associated date and time of creation is published internationally to certify its creation.[2]

How it's done

1. Each user of the IKR System either logs in (if previously registered) or provides an email identifier (e.g. an email address) to enable the IKR system to send the user the generated IKR record(s) and associate the file with its source.
2. The user then identifies the digital files or the file directory for the generation of IKR records and the IKR records are generated on the user's device. Each IKR record is associated with its file name, size and source of origination (IP address).
3. To generate the IKR record the IKR System employs a proven and reliable mathematical hash function[3], SHA-2, on the file or the contents of the chosen file directory to create a secure digital "fingerprint" of the contents.

But, as a further precaution, the IKR System concurrently calculates a second hash value using another SHA-2 hash function, then combines the two hash values thereby generating a truly unique identifier – an IKR record - for each file.

At the same time, IIPCC records the date and time the identifier was created and will publish the IKR record, as well as its associated date and time of creation, internationally to a number of patent offices and intellectual property authorities

---

[1] In the form of a digital file which can be, for example, a work created on a computer or a digitized file of a physical work (e.g. a digital rendering of the object, a digital photograph of the object or a digital recording of a performance, musical or film work).

[2] Please note that IKR can only authenticate existence of work expressed as a digital file. It cannot authenticate any other media used in expressing a work.

[3] A hash function is any function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called hash values. See: http://en.wikipedia.org/wiki/Hash_function

for their records.

Benefits

All this yields several important benefits.

As a real-world fingerprint cannot be used to re-generate the person from which the fingerprint came, the unique identifier –i.e. the IKR record - created by the IKR system cannot be used to re-create the digital document that produced it.

Any change to a file will be reflected in a change in the value of the IKR record, thus a file's IKR record can also be used to determine whether a file has been tampered with.

The IKR record, along with its corresponding date/time stamp, validates the authenticity of the asset, records the date and time of the creation and provides conclusive proof that is critically valuable, for instance, in subsequent litigation or dispute resolution proceedings.

In short, IKR improves the reliability and defensibility of your electronic records,

Furthermore, as the IKR record is held by neutral third parties, this helps to reinforce the impartiality of or eliminate potential conflicts that other bodies who might be tasked with the resolution of disputes, prosecution or even record keeping, might be unwillingly saddled with thereby helping these impartial third parties to do their jobs better with even greater credibility.

As more content is generated on computers, the ability to continuously – or incrementally authenticate files (with an IKR record) grows.