



## Content Authentication Platform

BayTSP's Content Authentication Platform (CAP) is an innovative system that utilizes multiple fingerprint and watermark technologies to monitor for and prevent copyrighted materials from being illegally shared on the Internet. In addition to using these recognition technologies, the Platform allows content owners to manage copyrighted materials from one location, using customized business processes that are applied wherever the content appears, providing a platform to build new business opportunities.

### The Benefits

The following are just a few of the benefits you receive when using BayTSP's CAP:

- The combination of fingerprinting and watermarking technologies work together to increase overall accuracy and effectiveness when monitoring for your copyrighted materials when they appear online.
- 24/7/365 operation, including a team that reviews possible infringements that fall outside the established business rules.
- Flexible deployment options



### Overview

The CAP is a platform that is open to different media content recognition technologies. Apart from aggregating recognition technologies, the CAP provides a single point of reference to owners of content and operators of websites to manage their content recognition needs in a centralized, consistent manner across multiple sites and applications.

The benefits of aggregation of different recognition technologies in this manner include the following:

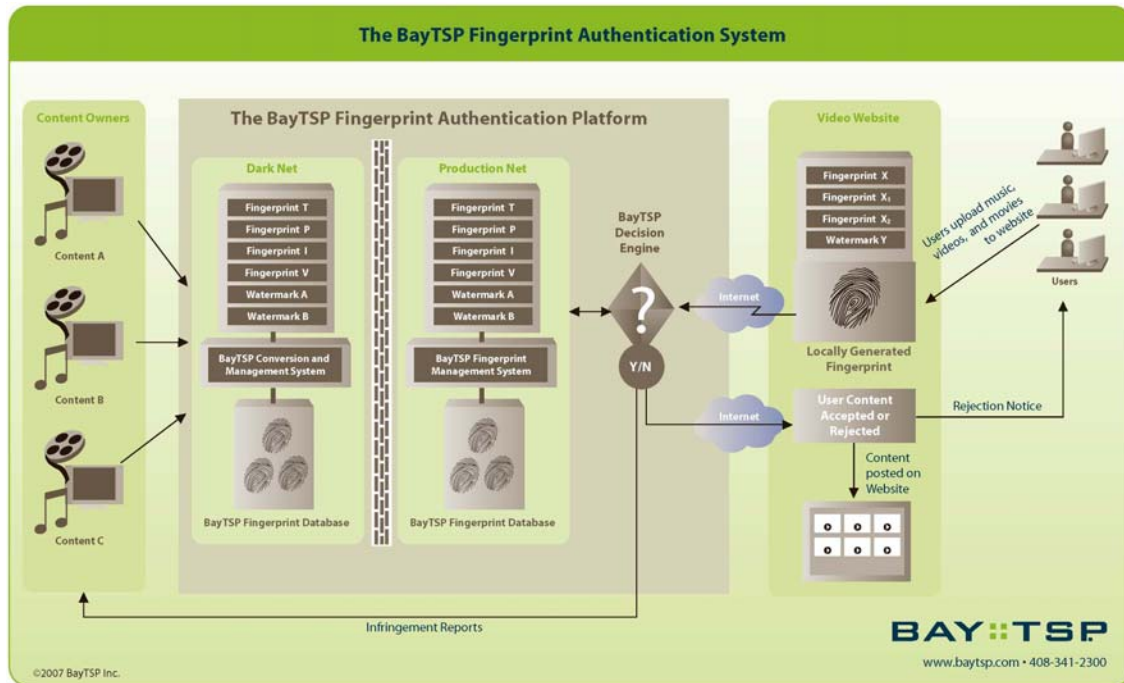
- Combined operation of technologies increases overall accuracy and effectiveness and provides flexibility in deployment.
- Integrates human review into the workflow process to further improve accuracy and confidence; and
- Control over fingerprints or watermarks is architected into the platform.
- Comprehensive coverage can be rapidly deployed and conveniently maintained across technologies.

# BayTSP Content Authentication Platform

## Applications of the CAP Platform

The CAP allows the immediate deployment of fingerprinting or watermark technologies by user-generated content (UGC) sites to filter user uploads for copyright material. UGC sites benefit by having access to a comprehensive set of fingerprints and the latest technology in a single service.

The following diagram illustrates the overall architecture of the CAP:



## How it Works

- Content owners generate fingerprints and watermarks of their copyrighted content with a system on site, or having BayTSP process the content for them. If BayTSP manages the fingerprint or watermark generation process, the original content is provided by owners and maintained in the DarkNet. It is in the DarkNet where fingerprint and watermarks are generated. Content owners can use multiple technologies (fingerprint or watermark) to create many fingerprint references per asset.
- A copy of all fingerprint or watermark files is kept on the production server. The firewall prevents the possibility of the original content or fingerprint files on the DarkNet from reaching the outside.
- The website accepting a user submission processes the file to create fingerprint information about that content.
- This information is transmitted to the BayTSP Decision Engine for a match within the BayTSP database.

## BayTSP Content Authentication Platform

- If a match is returned the result is passed directly back to the website to release the transaction to the next step in the website's workflow.
- Depending on how the hosting site configures its content filtering system, user generated content is prevented from appearing online until approved by the Content Authentication Platform, or it is removed shortly after appearing if the system identifies the clip as infringing on a client's copyright.
- When the content recognition technologies are unable to definitively make a clear, unambiguous determination whether or not these particular materials meet criteria, BayTSP personally deals with these cases.
- The content recognition technology can be deployed separately with a BayTSP device integrated into the website operation, or with an external BayTSP device. In either case, the CAP is integrated into the workflow and index of the website.

### Combined Technologies Increase Accuracy

The ability to combine different technologies together in a platform increases accuracy in detections. This is not only the result of different fingerprinting developers use different technology approaches, but also by using video fingerprinting in combination of audio fingerprinting. This combination is required to detect whether the original audio (or one of the original for assets with foreign language tracks) is included with the corresponding video. If the audio track is not one of the tracks associated with the video and not comprising of other copyrighted material, this could raise a fair use question and a possible response available in the platform would be to send the clip for human review.

### Controls Architected Into the Platform

The CAP provides a place for content owners to centrally manage in a secure, offline environment all their content they want used in the available fingerprinting technologies. This prevents the release of multiple copies of content and fingerprints to any number of different vendors and is designed so that content owners have full transparency and maximum control over the use of their fingerprints.

Website operators benefit by allowing the creation of trusted and auditable metrics that enable the development of activity based business models.

### Integrates Human Review Process

No matter how well tuned identification technologies are, there will always be a need for human review. This is not only to ensure that the technologies are performing as expected (or stay properly "tuned"), but also to handle identifications which have not been previously encountered and for to which the technology engine has been tuned, especially in an area where there is constant user innovation. While technology can provide scale to handle large problems, if it is not properly monitored, it can also make large problems even larger.

### Importance of Fingerprints - Coverage

The size of the fingerprint database is critical to the success of any deployment of fingerprinting technology. Without a comprehensive library of fingerprints, content will not be identified and the technology will at a practical level appear to be a failure. However, preparing and maintaining large comprehensive libraries is also a difficult and resource intensive effort, especially if there is a desire to generate fingerprints for a large number of emerging technologies and to bring new technologies online quickly in the future.

Fingerprint libraries can be created on an ad hoc basis without access to original content by taking samples of clips that have been distributed on video streaming sites or other sources. However this is problematic for a number of reasons.

- The quality of these underlying clips is not consistent, even though the resultant clips posted on websites is at the point of consumption in a standard format.
- It lacks completeness and will take an indeterminable period of time to completely obtain. For episodic content, this is a particular concern, particularly if the libraries extend across many seasons and may never be complete if obtained only in such a manner.
- Difficulty to obtain complete samples of individual pieces of content, as many of the clips seen are short extracts.
- Inconsistently applied metadata associated with the clips with reliance being placed on the identification by the user that posts this material, or by a laborious manual matching process that is subject to error and misidentification.



Revised 8/07