JUTEL

BUSINESS FINLAND

Beyond the Limits of PQC

PQC in Media Production and Distribution

Information security challenges in media production have increased significantly due to cybersecurity attacks, synthetic or misleading media, and AI-based media production.

Media systems often rely on networked and cloud-based infrastructures, making cryptographic mechanisms critical for protecting content throughout its lifecycle. The transition to post‑quantum cryptography introduces new considerations for media production, distribution, and authenticity.

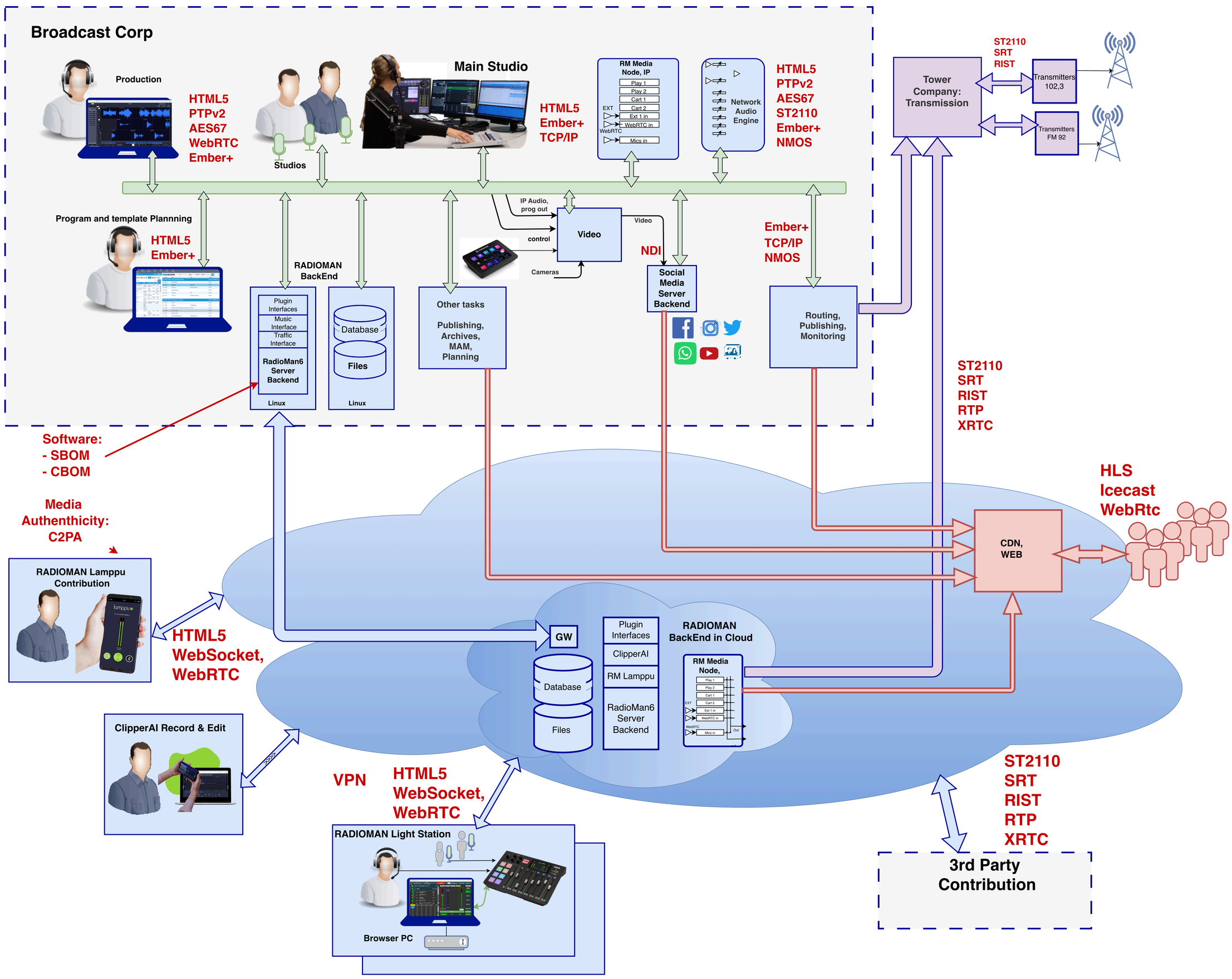
Initially, digital media production challenges were mainly technical and related to digital signal processing, media transmission between devices over networks, and device control. In the de facto standards developed for these purposes, information security and PQC resilience are not yet particularly advanced.

As media production transitions to network- and cloud-based environments, new standards have emerged for device control, media transmission between devices, and verification of media authenticity. These standards need to, and are evaluated from the perspective of **PQC** and data security in this project.

For media transmission over IP networks, traditional standardized methods have been used, including streaming protocols such as **RTP, SRT, RIST, RTSP, HLS, DASH, XRTC**, and **WebRTC**,and file transfer protocols such as FTP and HTTP. From a standardisation perspective, the industry standard protocols Secure Reliable Transport (**SRT**) and Reliable Internet Stream Transport (**RIST**) are key technologies for reliable media transmission. A similar, partly overlapping standard is WebRTC.

Device control typically relies on TCP/IP-based protocols or protocols operating over HTTPS, such as **Ember+**, which is used for media control, or MQ message-queue applications. In recent years, the SMPTE organisation has introduced the **ST 2110** standard family for professional audio and video media transport. For media transfers, precise timing is critical and the **PTP v2** is generally used in media production environments

More and more media production is done in Containerised Cloud environments where media transfer delays play important role. In order to avoid delays, new architectures with Common Memory Sharing like **MXL** have been developed. MXLrefers to the Media eXchange Layer of the **EBU** (European Broadcasting Union) reference architecture.



At the time of writing, the most commonly used media production device control protocol, **Ember+**, is entirely based on external security mechanisms and will likely evolve in the future.

The ST 2110 standard itself does not address device discovery or device control. For this purpose, the Advanced Media Workflow Association (AMWA) has developed the Networked Media Open Specifications (NMOS). **NMOS** is an open-source set of protocols and associated software for discovery, registration, connection, and management of ST 2110 networks.

To address the issue of media content provenance and authenticity, the Coalition for Content Provenance and Authenticity (**C2PA**) initiative has been introduced.The aim is to enable the tracking of media assets back to their original sources, including any changes made to the content. When creating and modifying media content, provenance data is generated, digitally signed, and added to the media asset as metadata.

The provenance data contains assertions statements covering areas such as asset creation, edit actions, and capture device details as well as previous provenance data thereby cascading the history of the asset. The provenance data is signed using PKI and the X.509 format. As a result, a subsequent user (a media producer, either a device or an organisation) or an end user can verify the origin and history of the contentthrough a validation service.

Within this project, the idea has emerged to monitor software structures and cryptographic structures in media production systems more closely using the concepts of Software Bill of Materials (**SBOM**) and Cryptographic Bill of Materials (**CBOM**). In the future, it may become common that media production system services are delivered with SBOM and CBOM documentation in a manner similar to ingredient lists on food packaging, enabling customers to track updates and changes related to information security.

www.jutel.fi

Jorma Kivelä, Jutel Oy, jorma.kivela@jutel.fi. phone +358 50 5554803
Ville Ollikainen, VTT, ville.ollikainen@vtt.fi phone +358 20 722 6017

www.pqc.fi