# Early Concepts of Multi-Trust Digital Timestamping: A Precursor to Hybrid Signature Architectures

Masamichi Tateoka
Independent Researcher, Japan
m8tateoka@googlemail.com

November 2025

**Abstract**

This technical note revisits two Japanese patent applications, JP2007-104024 and JP2009-274905 (granted as JP4929340)[5], which proposed timestamping systems resilient to key rollover and trust authority failures. These systems introduced mechanisms to preserve long-term digital proof by combining multiple independent trust anchors and computing the logical OR of validity intervals, enabling continuity of verification across key updates and trust authority changes.

Although these inventions were originally described within the operational domain of timestamping services, their underlying ideas anticipated the principles that now underpin modern *hybrid signature* architectures for the post-quantum transition era, where multiple cryptographic proofs are combined to mitigate single-point cryptographic failure. This paper highlights the historical and conceptual continuity between operational redundancy in early timestamping systems and cryptographic redundancy in today's hybrid signature models.

## 1 Introduction

The migration to post-quantum cryptography (PQC) has renewed interest in hybrid signature architectures, which combine multiple digital signature schemes to ensure resilience against future algorithmic vulnerabilities. While hybrid signatures are generally discussed as a new response to the PQC transition[3, 4], conceptual antecedents can be found in early studies on long-term timestamping and trust-chain continuity[5, 7, 6, 1, 2].

This note focuses on two early Japanese patents—JP2007-104024 (filed 2007) and JP2009-274905 (filed 2009, granted as JP4929340)—that introduced mechanisms for maintaining digital trust across key rollovers and trust authority updates.

We reinterpret these mechanisms in light of today's hybrid signature models, highlighting how ideas from operational timestamp management anticipated cryptographic multi-root trust designs.

## 2 Background: Trust and Longevity in Digital Proof

Long-term validity of digital evidence has long been challenged by key expiration, algorithm obsolescence, and the potential failure of certification authorities (CAs) or timestamp authorities (TSAs). The 2000s saw the emergence of timestamp-based long-term validation systems defined in standards such as RFC 3161 (TSP)[5], RFC 4810 (LTA requirements)[7], RFC 4998 (Evidence Record Syntax)[6], and ETSI specifications for XAdES and PAdES[1, 2]. However, most implementations relied on a single TSA and a single signature algorithm. JP2007-104024 and JP2009-274905 extended this model by introducing redundancy and recovery mechanisms to preserve proof validity despite key or authority changes.

## 3 Summary of JP2007-104024

The 2007 invention proposed a timestamp acquisition and management system that automatically detects key updates in a TSA and recalculates consolidated hash values of all unverified timestamps. Upon key rollover, a new timestamp is issued over the accumulated hash, effectively linking past and present signatures. This mechanism ensured continuity of verification even when the original signing key was retired or replaced. It also described cooperation among multiple TSAs, where one authority could timestamp the certificate hash of another, forming a multi-authority trust web.

## 4 Summary of JP2009-274905 (JP4929340)

The 2009 invention generalized this concept by formalizing the use of multiple timestamps and defining the *logical OR* of their validity intervals as the provable period of existence. This design anticipated redundancy-based verification: as long as one timestamp remained cryptographically valid, the associated digital evidence retained proof of existence. It also incorporated mechanisms for automatic re-timestamping upon key update events.

## 5 Conceptual Link to Hybrid Signatures

Modern hybrid signature schemes (e.g., ECDSA + Dilithium) achieve cryptographic redundancy by combining proofs from independent algorithms, where validity is

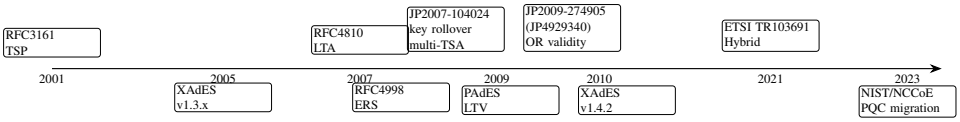


Figure 1: Milestones from timestamp LTV to hybrid signatures.

established through AND or OR verification logic[3, 4]. This parallels the operational redundancy introduced in the 2007–2009 timestamping systems: multiple independent cryptographic assertions (timestamps or signatures) jointly ensure continuity of trust even when one component becomes obsolete or compromised.

Thus, these early patents effectively anticipated the architectural philosophy of multi-rooted digital trust: resilience through diversity and redundancy.

# 6 Discussion and Implications

The continuity between timestamp-based redundancy and cryptographic hybridization suggests that trust diversification principles were already well understood in the mid-2000s within timestamping infrastructure design. Recognizing these patents as early formalizations of multi-trust models provides historical grounding for contemporary PQC migration strategies.

# 7 Conclusion

Nearly two decades before the post-quantum transition, the concepts of multi-authority timestamping, key-update resilience, and validity-interval aggregation established the foundation for what is now called hybrid signature architecture. These early designs demonstrate that operational redundancy and cryptographic redundancy share a common goal: sustaining digital trust across time, technology, and authority changes.

# References

[1] ETSI TS 101 903 (xades) selected versions. ETSI, 2005–2010.

[2] ETSI TS 102 778-5 (pades) long term validation. ETSI, 2009.

[3] ETSI TR 103 691: Hybrid signatures for electronic trust services. ETSI, 2021.

[4] Migration to post-quantum cryptography. NIST NCCoE, 2023.

[5] Carlisle Adams, Paul Cain, David Pinkas, and Russ Zuccherato. RFC 3161: Internet x.509 pki time-stamp protocol (tsp). IETF RFC, 2001.

[6] Tobias Gondrom, Reinhard Brandner, and Ulrich Pordesch. RFC 4998: Evidence record syntax (ers). IETF RFC, 2007.

[7] C. Wallace, D. Pinkas, and N. Pope. RFC 4810: Long-term archive service requirements. IETF RFC, 2007.