

[Press Release]

2007.9.27

KDDI R&D Laboratories Inc.

A New Message Authentication Mechanism for Streaming Multimedia Contents  
~ Detect Invalid Broadcasts in Real-time Verification ~

KDDI R&D Laboratories Inc. has invented a new message authentication mechanism for streaming multimedia contents and developed a prototype system based on the mechanism; the system detects invalid or altered broadcasts in real-time verification and it is applicable for WANSEGU services (digital broadcasting service for mobile phones).

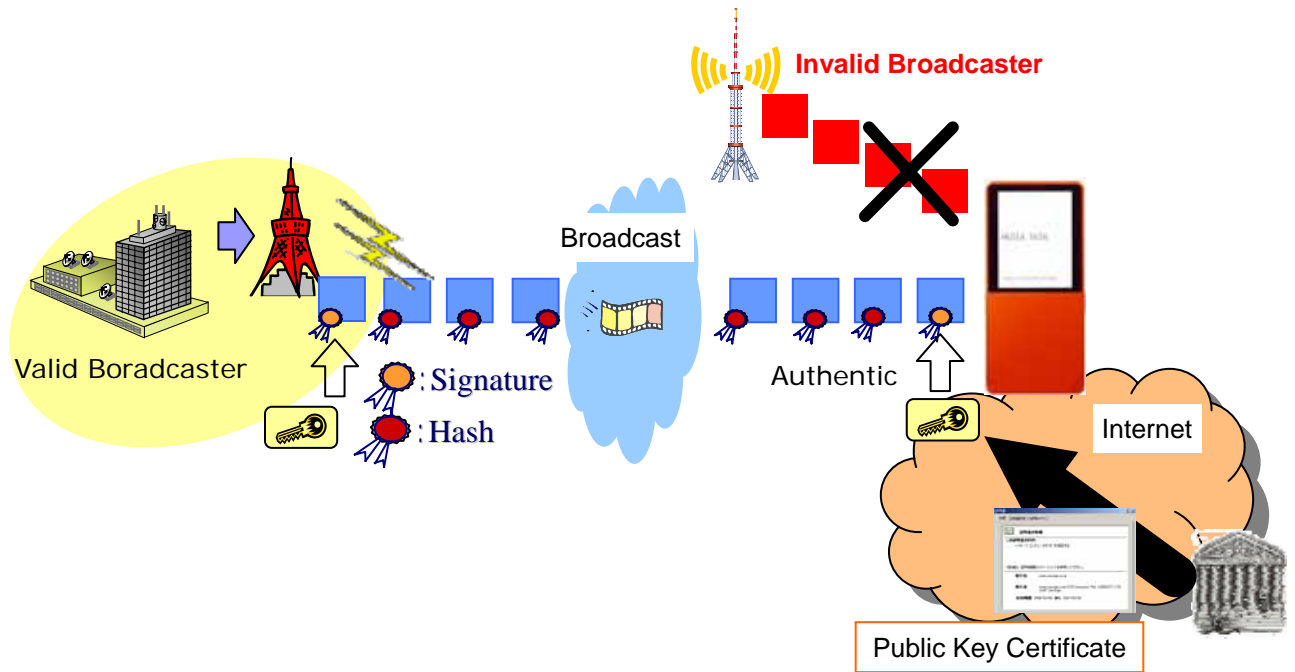
We have succeeded in developing the world's first system that realizes real-time verification of WANSEGU contents on mobile phones.

The system produces a lightweight verification function to low-power mobile phones even though the broadcast provides on a lossy channel. Broadcasters who use our system will produce secure programs to their customers without concern for malicious actions.

Essential flavors of our mechanism are as follows; a digital signature mechanism of the system consists of public key encryption algorithm and hierarchical structures of hash values, and the hash values and the signatures are stored in broadcast contents in an error-resistant fashion. These techniques have achieved lightweight and robust message authentication for broadcasting

We will consider new services using the system such as local-area broadcast services, IP-based broadcast services and emergency broadcast services.

(Appendix)



Overview of the system



Picture of the prototype System