FOR IMMEDIATE RELEASE

New Technology for Redacting Digitally Signed Documents, Developed Jointly by Hitachi and AIST, Has Been Adopted as an ISO/IEC International Standard

Ensures both privacy and authenticity of publicly released documents, contributing to a safe data-utilization society

Tokyo, August 26, 2024 – Hitachi, Ltd. (TSE: 6501, "Hitachi") and the National Institute of Advanced Industrial Science and Technology ("AIST") today announced that their jointly developed technology for redacting digitally signed documents ("redactable signature" technology) has passed final approval by the Joint Technical Committee 1 (JTC 1) of the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), gaining adoption in international standard ISO/IEC 23264-2. The two newly standardized schemes provide means for ensuring the authenticity (absence of falsification) of digitally signed documents when they are made public in partially redacted form.

The redactable signature schemes use digital technology to realize partial disclosure of documents while enabling detection of unauthorized alteration or falsification. The two newly standardized schemes provide an efficient means for partial disclosure of public documents, while enabling the authenticity of data related to product development, in fields such as pharmaceuticals and finance, to be guaranteed, without loss of data use convenience, even when a document has undergone sanitization (anonymization) for privacy protection reasons. They are thus expected to contribute toward a safe data-utilization society.

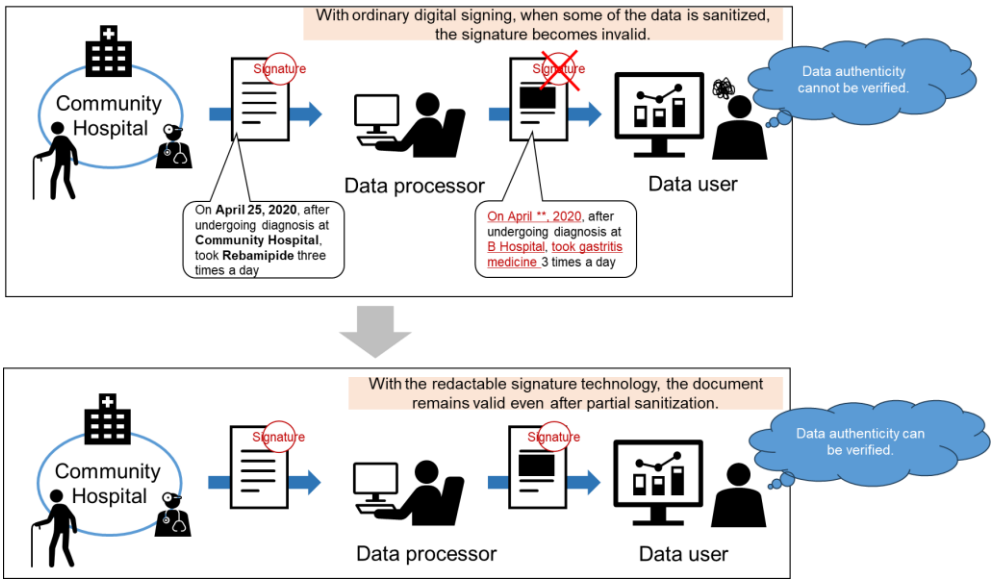

Figure 1. Example of redactable signature use with medical care data
(An example for pharmaceutical product development, with sanitization of personal and other information in the use of user data on existing products)

■ Background to the Standardization

Now that digital technology has come into wide use, proceedings that used to involve printed documents are being replaced by digital processes, giving all the more importance to digital

signature technology able to detect data alterations or falsification and guarantee data authenticity. As a current way of official document management, it is sometimes necessary to redact (erase or blank out) certain information for privacy or other reasons before publication or disclosure. With conventional digital signing technology, however, the act of redaction itself is regarded as falsification, invalidating the digital signature and making it difficult to guarantee the authenticity of a redacted document.

In addressing this issue, ISO/IEC JTC 1[*1] drew up international standard ISO/IEC 23264, “Information security—Redaction of authentic data” relating to the application of digital signature technology, with its expanding uses. To promote this standardization, Hitachi and AIST, starting some twenty years earlier, engaged in pioneering research and development on a digital signature technology for realizing redaction of documents by digital means (redactable signature technology). As a result of this joint development, two redactable signature schemes (MHI06 and MIMSYTI05) were adopted in international standard ISO/IEC 23264-2.

■ Features of the Standardized Technology

Using the redactable signature schemes, a signer can set redactable data blocks in advance at the time of creating a document and set each block as either disclosable or non-disclosable before public release. Moreover, the digital signature applied when a document is created can be used to verify a document that is partially non-disclosable, and to confirm that the document has undergone only legitimate editing. Furthermore, the redactable signature schemes adopted in the new ISO/IEC 23264-2 standard each have different additional security properties; and in the case of MHI06 and MIMSYTI05 jointly developed by Hitachi and AIST, both have the property of allowing documents to be edited multiple times and are able to control the disclosure scope divided into multiple levels.

MHI06 has the property of enabling multiple signed documents or data to be merged, within the scope specified in advance (Mergeability), and enabling the information in redacted fields to be hidden (Undetectability of redactions). This scheme is suited to uses in which the scope of signed data to disclose should be dynamically and efficiently changed, depending on the privacy protection policy and status.

MIMSYTI05 can add redactable signature functionality using any kind of digital signing method. It can be combined not only with such methods as RSA signature[*2] or ECDSA[*3] but also with quantum-safe signature methods. In addition, this scheme is suited to applications where documents are sorted by whether they contain redactions since it can detect the fact of redactions.

■ Looking Ahead

The redactable signature schemes were initially developed as digital technology for protection of public documents but are expected to find wider application not limited to that purpose, including for verification of the originality of partially released data. By combining this technology with sanitization technology, for example, it is expected to find wide use as technology achieving both privacy protection and data authentication. Hitachi and AIST will continue engaging in research and development on redactable signature and other cryptographic technologies, along with promoting their implementation in products and services, thereby contributing to realization of a safe digital society.

*1 ISO/IEC JTC 1: JTC 1: Joint Technical Committee 1 of the ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission)
*2 RSA signature: A digital signature method relying for its security on the difficulty of integer factorization problem
*3 ECDSA (Elliptic Curve Digital Signature Algorithm): A digital signature method relying for its security on the difficulty of the elliptic curve discrete logarithm problem

- End -

About Hitachi, Ltd.

Hitachi drives Social Innovation Business, creating a sustainable society through the use of data and technology. We solve customers' and society's challenges with Lumada solutions leveraging IT, OT (Operational Technology) and products. Hitachi operates under the 3 business sectors of “Digital Systems & Services” – supporting our customers’ digital transformation; “Green Energy & Mobility” – contributing to a decarbonized society through energy and railway systems, and “Connective Industries” – connecting products through digital technology to provide solutions in various industries. Driven by Digital, Green, and Innovation, we aim for growth through co-creation with our customers. The company’s revenues as 3 sectors for fiscal year 2023 (ended March 31, 2024) totaled 8,564.3 billion yen, with 573 consolidated subsidiaries and approximately 270,000 employees worldwide. For more information on Hitachi, please visit the company's website at https://www.hitachi.com.

About the National Institute of Advanced Industrial Science and Technology (AIST)

The National Institute of Advanced Industrial Science and Technology (AIST) is a national research institute with 12 research bases in Japan and approximately 2,300 researchers. It is one of the largest public research institutes in Japan that conducts research and development of science and technology. AIST's mission is to "solve social problems" and "strengthen industrial competitiveness." For this, our core technologies are bundled together in its 5 fields and 2 centers to demonstrate comprehensive capabilities, and it conducts R&D from a central and pioneering position in the national innovation system based on the national strategies formulated bearing in mind the changing environment regarding innovation. For more information, please visit the AIST website (https://www.aist.go.jp/index_en.html).

Contacts:

Hitachi, Ltd.
Research & Development Group
https://www8.hitachi.co.jp/inquiry/hqrd/news/en/form.jsp

National Institute of Advanced Industrial Science and Technology (AIST)
Cyber Physical Security Research Center
Contact Page: https://www.aist.go.jp/aist_e/contact/index.html

---

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
