

## Recordkeeping and digital signatures

*This Guideline provides advice to public authorities which send and receive records authenticated with digital signatures and explores some of the records management issues arising from the use of digital signatures.*

### Digital signatures, digitised signatures and electronic signatures

In Queensland, the *Queensland Government Authentication Framework* (QGAF) is the primary standard for establishing identity registration and authentication requirements for public authorities, with respect to their service delivery, privacy requirements, and risk assessments. The QGAF *Authentication Concepts* defines a digital signature as being “created by encrypting a message with a user’s private key, appending this to a copy of the original message and sending the aggregated message”<sup>1</sup>. The message is then decrypted by the receiver using the sender’s public key. This use of asymmetric cryptography when used within public key infrastructure (PKI), is useful in confirming that a record has not been modified in transit and authenticating the identity of the sender.

Digital signatures can be used to sign digital documents. As with other types of signatures, this may be done to identify the signatory and verify their approval of the content; and verify that no changes had been made to the content sent and being viewed by the receiver<sup>2</sup>.

Other electronic signing methods (using authentication other than PKI, such as passwords or biometrics) and digitised signatures (an electronic copy of handwritten signatures) are not digital signatures, and therefore out of scope of this advice.

### Public records authenticated with digital signatures

The *Public Records Act 2002* (the Act) and *Information Standard 40: Recordkeeping* (IS40) apply to records in all formats, regardless of the technology used to create, transmit or authenticate the record. Under Section 7 of the Act, a public authority must “make and keep full and accurate records of its business activities”. Full and accurate records have attributes of being adequate, complete, meaningful, accurate, authentic, inviolate, accessible and useable.

The use of digital signatures can assist public authorities in confirming that electronic records are authentic and inviolate. Due to the nature of the authentication process used in public key cryptography, certifying authorities issue public and private keys with certificates which may only have a limited validity period or be revoked. Adequate documentation and processes must be in place, to ensure that once the digital certificates authenticating the message have expired, the record is still valid. This can be done through the capture of relevant metadata and secondary records<sup>3</sup> relating to the digital signature.

<sup>1</sup> Office of Government ICT (2006) *Queensland Government Authentication Framework- Authentication Concepts* p.28

<sup>2</sup> NSW Government Chief Information Office (2005) *Authentication – Digital Signatures Guideline* p.4 [http://www.gcio.nsw.gov.au/documents/Authentication\\_0205.pdf](http://www.gcio.nsw.gov.au/documents/Authentication_0205.pdf) cited 25 March 2009

<sup>3</sup> Records created which relate to the digital signature but are not part of the primary message, for example the certificate validation response



All stages of the records management process (creating, capturing, managing and maintaining records, and lawfully disposing of records) will need to be considered for both the primary record and secondary records relating to the digital signature. These additional records are as important as the primary record, as they verify the integrity of the record.

A public authority should consider the purpose of the digital signature for the record, as this may affect the information about the digital signature which needs to be preserved with the primary record. For example if a digital signature is used by a client to provide a written consent, the records required and their retention periods may vary from those of a signature used to approve a building plan.

### **Recordkeeping compliance**

Some strategies for the use of digital signatures which may assist in meeting recordkeeping obligations are:

- determine internal policies and documentation standards relating to assigning and availability of keys within a public authority
- include a human-readable name of the signatory, date and time of the signing, intent of the signatory (purpose for applying the PKI digital signature) with the record<sup>4</sup>
- determine which digital signature transaction specific and associated records need to be kept, and their retention periods in accordance with an authorised Retention and Disposal Schedule. These may include:
  - digital signature, certificate, certification validation responses
  - PKI unique administrative records – certificate authorisation, subscriber agreement
  - other non-PKI records – operational procedures, training documentation<sup>5</sup>.
- register information about the digital signature, to ensure audit trails are maintained. This may be included as metadata in accordance with the *Queensland Recordkeeping Metadata Standard*
- identify who is responsible for maintaining accuracy and accessibility for long-term preservation of the record.

There are different ways to prove the source of a record, protect against forgery and maintain confidentiality, where required. If a public authority chooses to use digital signatures to achieve this, the challenges of the technology for records management must be recognised and reflected in the recordkeeping policy and systems of the authority.

---

For more detailed guidance on the management of public records visit the Queensland State Archives' website at <http://www.archives.qld.gov.au>, or contact us on:

Telephone: (07) 3131 7777

Email: [info@archives.qld.gov.au](mailto:info@archives.qld.gov.au)

---

<sup>4</sup> National Archives and Records Administration (2005) *Records Management Guidance For PKI Digital Signature Authenticated and Secured Transaction Records* p.11 <http://www.archives.gov/records-mgmt/policy/pki.html> cited 25 March 2009

<sup>5</sup> Ibid, p.13