

Archives Advice No. 7

Authentication Technologies and Recordkeeping

Considerations for Government Officials

What is Authentication and why is it needed?

As Internet usage continues to grow, agencies increasingly want to make more services available online. However, providing services via the Web requires consideration of many issues. One of the most important of these is authentication – making sure that customers are who they claim to be. When services are provided via traditional, non-electronic processes, various authentication methods are used. Customers are required to sign forms or letters, present identification numbers or case numbers, or show a driver's license or birth certificate. Most of these methods will not work online.

An agency may implement online authentication in a number of ways, including:

- Passwords, personal identification numbers (PINs) and user identification (USER IDs)
- One-time passwords;
- Challenge and response systems;
- Cookies;
- Biometrics;
- Conventional encryption;
- Pretty Good Privacy (PGP);
- Public key cryptography (digital certificates), and;
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

Each method or technology has its own strengths and weaknesses, including cost and ease of implementation and use. They may be used in combination. In addition, they have an impact on how we conduct business and the records we maintain.

Recordkeeping Implications

The need to manage records remains, whether those records are in an electronic, paper or other media. Records of an agency's business activities must be created and managed in such a way that they retain their integrity and remain accessible for as long as they are required by approved retention schedules. Agencies should consider how records subject to authentication and encryption processes will be managed and stored, taking into account privacy and security requirements. As certificates and keys expire, access to encrypted information may be compromised while software obsolescence and the degradation of storage media may also affect data integrity and accessibility. To mitigate the impact of encryption software obsolescence, agencies should store information unencrypted but in a suitably secure electronic environment to ensure continued accessibility, rather than maintain the information in encrypted form in an



GEORGIA ARCHIVES

insecure system. Such information may be required and linked with records documenting the authentication and encryption processes in order to verify its reliability. Records documenting the authentication and encryption processes will include digital certificates, digital signatures, subscriber identity, time and date stamps, revocation checks and message verification.

Implementation Considerations

In developing a case for authentication technologies, agencies will need to consider some important business continuity issues, particularly where information is encrypted. An agency's ability to continue business might be severely hampered if the information cannot be accessed for some reason. If the information is maintained in encrypted form and can only be accessed by decrypting it with the agency's private key, what happens if that key is held by a staff member who is on leave, sick, overseas, or just cannot be contacted? Agencies must also plan for the loss of passwords and the forgetfulness of staff when needing access to private keys without which the information is inaccessible.

In addition, privacy concerns must be addressed during the planning phase of selecting an authentication technology. The agency must be able to comply with the requirements of the Georgia Open Records Act for the protection of personal data.

Agencies should adopt a risk-based approach and consult their records manager to develop appropriate management strategies for addressing all recordkeeping concerns. If you need further assistance, please call the Georgia Archives at (678) 364-3790.