Fact Sheet

Cogito Group

Digital Signatures

Digital Cryptographic Signatures

A digital signature is an electronic, encrypted, stamp of authentication on emails or electronic documents. A signature confirms that the information originated from the signer and has not been altered since then.

Digital credentials are the digital equivalent of a person's signature on a piece of paper. They can also act as a digital version of identity documents issued by trusted parties such as government institutions. They are used to establish a person's privileges, characteristics, and identity in the electronic world and can be used to interact with that electronic world.

Enhanced Security Benefits

Operating a Certification Authority that is used for more general purposes allows for more flexibility in what types of certificates can be issued without potentially affecting certification or the security of a larger ecosystem.

The issuance of certificates confirming an individual's identity, with appropriate identity proofing and certificate policies in place, enables you to verify a staff member's association with the institution.

These certificates and keys can then be used for digital signing of emails and other documents. The inclusion of a digital cryptographic signature on a document or communication would allow staff, as well as the general public if the root CA is included in trust store programs, to verify that it has come from a person that has been verified by the institution.

This capability has the potential to greatly reduce the effectiveness of spam and phishing attacks within your institution. By allowing the end user to assert the authenticity of the signature and the document to which it's attached this provides a factor to positively identify official communications and documents that works alongside existing spam controls and user education.

Additionally, assuming the certificate's private key is kept secure and accessible only to the end entity, this provides a non-repudiation capability for incidents of dispute. That is, if an email is signed by a specific certificate's private key then it can be said with confidence that the holder of that certificate is the only person that could have generated that signature. The association between the certificate holder, the signature, and the signed object cannot be later denied.

Digital Signatures

Fact Sheet

Four Pillar Assurance

A certificate authority issues and verifies digital certificates and provides the following assurances:

Non-Repudiation

Evidence, verifiable by a third party, that a transaction has been sent or authorised by the purported sender. Digital signatures bind the identity of a party to the transaction so that knowledge of the transaction cannot later be denied.

Authentication

The process of testing or verifying an assertion, in order to establish a level of confidence in the assertion's reliability.

Integrity

Digital signatures can be used to prove that data has not been tampered with in transit. This is important in its own right, but also for non-repudiation.

Confidentiality

Digital signatures obligate the recipient or holder of the information to not disclose it to other parties.

Uses Cases

Digital signatures can be utilised in a multitude of cases, including:

- For logical access to systems.
- For physical access to sites and facilities (supporting backwards compatibility with the current solution door and barrier solution, but it is working towards a more secure physical access solution).
- Electronic signature of email.
- Electronic signature of forms.
- Electronic signature of financial transactions.
- Electronic signature of approvals.
- Access to web site portals.
- Access to web-based systems.
- Binding their use to a particular function. For example, a private key can be generated that will only allow signature operation and not decryption.

Digital Signatures

Fact Sheet

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.