



Authentication - Digital Signatures Guideline

Issue No: 2.2

Issue Date: June 1999

Review Date: February 2005

Table of Contents

1. Purpose and Scope	2
2. Introduction	2
2.1 Key Points.....	2
2.2 What is Authentication?	2
3. Using Authentication	4
3.1 Purposes	4
3.2 Outline Process.....	4
3.3 Agency Roles	6
3.4 Trustworthiness - Relying Party Perspective	6
3.5 Trustworthiness - Subjects' Perspective	7
3.6 Associated Functions	8
3.7 Liability.....	8
3.8 Standards.....	8
3.9 Project GATEKEEPER	9
3.10 Australian Business Number - Digital Signature Certificate (ABN-DSC) ...	9
4. Agency use of Authentication	9
Glossary	10

Table of Figures

Figure 1: [Validating PKC via the Internet](#)

1. Purpose and Scope

The purpose of this Guideline is to provide information to NSW Government agencies about authentication and its use. It is focussed on the use of digital signatures.

2. Introduction

Authentication is a means to providing trustworthy electronic commerce or electronic service delivery. It is also a tool for IM&T security, particularly for ensuring the integrity of information and providing access control.

This Guideline concerns authentication involving one particular type of "electronic signature" - "digital signatures" using "public key certificates" (PKC). These use asymmetric cryptography and trusted authorities. A glossary is attached.

The NSW Parliament passed the Electronic Transactions Act in April 2000. This Act is the uniform Bill agreed between the States and Territories. It gives Electronic Signatures the same legal status as personally written signatures for most purposes and establishes that the use of an Electronic Signature means that the signer approves the content of the 'document' being signed. However, the Act does not define any characteristics for a legally acceptable electronic signature.

Authentication is also part of access management for ICT systems, and PKC may be used in this role if security risks are assessed as high. The underlying technology, asymmetric cryptography, may also be used to encrypt information. These uses are not addressed in this Guideline. However, they may help to defray costs and or extend the benefits of electronic signatures.

2.1 Key Points

Electronically signed documents must use digital signatures that are:

- Uniquely linked to the signatory;
- Capable of identifying the signatory;
- Linked to the signed document in such a way that any subsequent change to the document will be detected.

2.2 What is Authentication?

In this Guideline authentication is a means of:

- Preventing undetected modifications to an electronic document;

- Providing limited, but reliable, information about a person;
- Providing other functions of a signature in an electronic environment, in particular the signer indicating approval of the signed document.

This authentication comprises:

- A digital signature relying on asymmetric cryptography;
- The infrastructure for authenticating information about people and systems;
- The mechanism for binding a signature to a digital document.

A [document](#) could be any type of digital data file, for example text, CAD model, digital video, digital sound recording, etc, and its presentation to people could be multi-media combination of different types.

Digital signatures rely on asymmetric cryptography, popularly called [public key cryptography](#). This involves a pair of cryptographic keys, one to encrypt information, the other to decrypt it. By managing who has which key, many people can send digital items that can be used by only one person, or one person can send an item that can be used by many people. The key that is made available to many people is usually called the [public key](#), the other is the [private key](#). Note that either key can encrypt and decrypt, but neither can decrypt what it encrypted. Keys are issued to signatories as an authentication package including a certificate.

The most common type of authentication certificate is an [identity certificate](#), widely called a [public key certificate](#) (PKC) and internationally standardised. This identifies the [subject](#), the person who uses it to sign a [document](#). When identity is important the thoroughness of the processes used to confirm it becomes an issue. The subject does not have to be a human person, it could be a computer or an organisation, although such entities would usually be signing in accordance with an instruction from a real person.

A second type of certificate is emerging - an [attribute certificate](#) (AC). This says something about its subject, for example their address, occupational qualification or licence, authority, role, clearance, right to a benefit, etc. It is expected that some types of attribute will become standardised. AC standards have been internationally agreed. They do not provide digital signatures although they may be bound to a PKC that does, and may be provided as an extension to a PKC.

Asymmetric cryptography is computationally intensive so it is rarely used to encrypt more than a few dozen bytes of data. This means that it is not used to encrypt [documents](#) for confidentiality purposes. However, the third type of certificate - [key certificates](#) - are used to encrypt the secret keys for symmetric cryptography and short messages used in the banking industry. This Guideline is not concerned with such uses.

3. Using Authentication

3.1 Purposes

Digital signatures can be used to sign digital documents. The usual purposes of signing documents are to:

- Identify the signatory;
- Provide certainty about the signatory's personal involvement in the act of signing;
- Associate the signatory with the content of a document;
- Attest the intent of the signatory to endorse or approve authorship of a text;
- Attest the intent of the signatory to associate themselves with the content of a document written by someone else;
- attest the fact that, and the time when, the signatory had been at a given place.

A digital signature created with a PKC and private key issued by a trusted authority should be acceptable for all these purposes apart from the last. Place is always an issue in the virtual world, but could be attested to by another person in the same place at the same time. Time could be similarly treated, although trusted time stamping services are emerging.

Attribute certificates could be appropriate when having a particular attribute (or privilege) is a requirement for doing or receiving something. The reliability of such certificates would depend on the trustworthiness and authoritativeness of the issuer, and the processes they use to establish that the subject has the claimed attribute.

3.2 Outline Process

Using an authenticated digital signature typically involves the following steps summarised in the figure below:

1. The person wanting to digitally sign something must first acquire a PKC and private key from a [Certification Authority \(CA\)](#). This process would normally involve them proving their personal or corporate identity if they were unknown to the CA. PKC and key can be downloaded via Internet from CAs around the world, however, it is generally agreed that smart cards are the most suitable media for them.
2. The holder of a PKC signs digital 'documents' as required. Typically the mechanism is provided by a software package that they invoke and requires them to validate that they are the legitimate subject of the PKC. If the software is on a smart card then a card reading device will be needed. The underlying steps are:

- The "document" is "hashed", this is a algorithmic process that adds up the numeric value of the bits in the document. If a single bit is changed, added or deleted then the hash value changes.
 - The hash value is encrypted using the signatory's private key to create a digital signature.
 - The "document", ie data file, digital signature and a copy of signatory's PKC are sent to its recipients.
3. Each recipient processes the digitally signed 'document' using software to:
- Decrypt the digital signature using the signatory's public key from the PKC, to reveal the hash value. The signer's PKC usually accompanies the signed document, although for some transactions it may be more appropriate to leave it in a repository.
 - Calculate a new hash value (the PKC provides details of the algorithm) and compare it with that produced by the signatory. If they are identical then the 'document' has not been illicitly modified.
 - If necessary validate (via Internet) the PKC with the purported issuing CA, including checking their [Certificate Revocation List](#) (CRL) repository or using a service provider to establish that a PKC is unrevoked.
 - Optionally, check any policy statements or references in the PKC to establish its suitability for the relying party's purpose. This is a risk management matter.
 - If the CA is unknown to the recipient then they may seek information about them and their processes to determine whether or not they are trustworthy for the recipient's purposes, (via Internet to look at CP & CPS, see below).

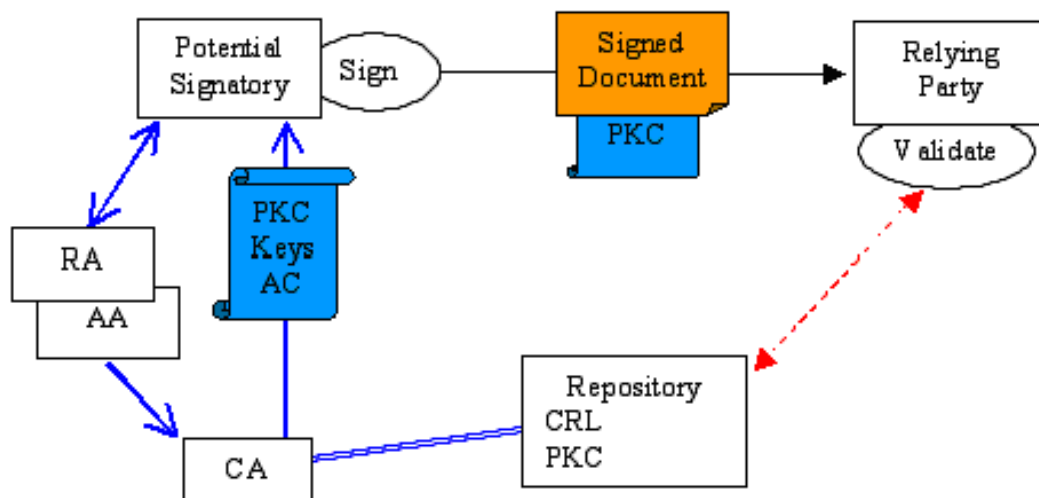


Figure 1: Validating PKC via the Internet

PKC are issued with a period of validity. This means that the subject's use of the digital signature is valid in this period, unless the PKC is revoked. A signed 'document' may have a 'life' far beyond this period of valid signing. The digital signature does not become invalid when the PKC's period of validity expires. However, if many years go by technological advance may mean that it becomes theoretically possible to change the 'document' and then apply a fraudulent signature. The status of a digital signature when the PKC issuing CA ceases business is unclear.

3.3 Agency Roles

Agencies may have one or more of the following roles with digitally signed "documents" or attribute certificates:

- As recipients of digitally signed documents or attribute certificates. This role is that of [relying party](#).
- Their organisations, staff or systems may be subjects holding PKC or attribute certificates that they use during their work for the agency.
- As issuers of PKC or attribute certificates, to their own organisations, staff or systems, or to external ones.

There are three possible roles associated with issuing certificates:

- Registration Authorities (RAs), who establish the identity of potential certificate subjects.
- Certification Authorities (CAs), who issue PKC (using the information provided by a RA) and operate the certification service. They may also issue attribute certificates.
- Attribute Authorities (AAs), who certify attributes and may be the custodians of particular attributes. They may also issue attribute certificates.

Agencies could be RAs, CAs or AAs, particularly with respect to their own staff or those of other agencies. Some agencies could be AAs for particular attributes amongst the wider community. A few agencies may have the infrastructure, outlets and staff skills, that makes them potential RAs for the wider community.

3.4 Trustworthiness - Relying Party Perspective

Relying parties are most concerned about trustworthiness of certificates. The areas of possible concern are:

- Fitness for purpose, certificates may be issued for specific purposes using systems and practices appropriate to them. Accepting a certificate issued for an inappropriate purpose may be a risk. Purpose is set out in CAs'

- published Certification Policies (CP), which will also govern the RA's activities.
- The reliability of hashing algorithms and strength of encryption used to create digital signatures. Providing standard algorithms are used there are negligible risks with hashing or asymmetric encryption.
 - There is no such thing as guaranteed proof of identity, although the degree of rigour in RA practices can make fraudulent identity more or less easy. Some RAs may offer levels of proof similar to the points systems for passports or opening bank accounts. Rigour in identity proving is a function of the purpose stated in the CP.
 - The CA/RA (or AA) and their operating practices are a matter for trust. The latter, typically covering procedural, technical and security aspects, are published in Certification Practice Statements (CPS).

Whether the secret key was under the sole control of the signatory, this may be a particular issue for a PKC used by a person in their personal capacity. If the secret key is not under their sole control then a Court may accept their repudiation of an instance of its use. A secret key stored on a PC hard disk or in a networked system is almost certainly not under the sole control of the signatory.

Wider concerns about trustworthiness may also exist, "do they really do what they say they do?", although in the case of a major "household name" CA these may be minimal. There are two broad approaches to this issue. First the idea of a chain of trust stretching from some "root CA" through layers of CAs, each certifying CAs in the level below; the theory being that untrustworthy collusion becomes very difficult. A variation on this is a web where many CAs certify each other. The second approach is akin to quality certification, independent external assessing bodies audit CAs against standards and the CAs' CP/CPS.

These approaches are not mutually incompatible. Project GATEKEEPER is an example of the second, but neither are yet in place in Australia. Some form of national certification regime for CAs is expected.

3.5 Trustworthiness - Subjects' Perspective

Privacy is likely to be the major concern, although confidence that a subject cannot be imitated or their identities stolen could be others. Both of these are issues for CAs to address in their CPS. One specific aspect of a subject's privacy is any list of relying parties created by queries to a CRL for the subject's PKC. The general trustworthiness of CAs and the reliability of hashing and encryption to prevent fraud may also be issues. Both are discussed above.

3.6 Associated Functions

Most packages add a printable statement that the document has been digitally signed with details from the PKC or attribute certificate. Additional features associated with digital signatures could include:

- Appending the scanned image of the signatory's handwritten signature to a document when it is digitally signed;
- Trusted time notarisation stamping involving certified time from a trusted authority being added to a signed document.

The [paper signature](#) analogy can inhibit the creative use of digital signatures for authentication. For example:

- Authenticating messages between unattended devices; [signed](#) reports or instructions between devices can be communicated via Internet with assurance that false ones can be rejected;
- Providing a means of showing that a web page is authentic and not a 'spoof' or worse;
- Signing entries in a directory or database.

For purposes such as access control a PKC may need to be bound to a person by something other than (or in addition to) their accepted identity - name being the well established meaning of 'identity'. A biometric characteristic, unique to a particular person, provides a highly reliable means of binding a PKC to the physical person. [Biometrics](#) also provide a means, alternative to PIN or password, of verifying that the PKC holder is the PKC subject. Because a biometric characteristic is unique to a specific person it has the potential to detect subjects with more than one identity in a database. Any use of biometrics requires appropriate devices.

3.7 Liability

Attention is drawn to the report to the National Electronic Authentication Council at http://www.agimo.gov.au/data/assets/file/12284/PKI_legal_report_May2002.pdf

3.8 Standards

Agencies adopting authentication are to use PKC complying with the X.509 version 3 recommendation. Hashing and encryption algorithms are also to comply with national or international standards.

Agencies are not to create their own extensions to X.509 certificates

3.9 Project GATEKEEPER

The Government Public Key Authority, and its CA(s), are a Commonwealth initiative to provide highly trustworthy PKC for use by Commonwealth agencies. As relying parties NSW agencies could accept PKC from these CAs. Some NSW agencies may use PKCs from these CAs providing the associated Certificate Policies are appropriate and acceptable from a risk management perspective, appropriate for their own staff or other purposes. When acquiring CA services from a Gatekeeper accredited supplier agencies should ensure that there is no weakening of the CPS that enabled accreditation.

3.10 Australian Business Number - Digital Signature Certificate (ABN-DSC)

ABN-DSCs are issued to business entities as a consequence of the New Australian Tax System, however, they should not be confused with the PKC initially issued without a publicly accessible CRL. As relying parties, agencies may find that ABN-DSCs are appropriate for their purposes.

4. Agency use of Authentication

Authentication is a mechanism for IM&T security. Agencies are strongly encouraged to use authentication appropriately as part of their electronic service delivery, other electronic commerce activities and general IM&T security. This use, in increasing order of cost, could be:

- As a relying party - no cost apart from instituting internal procedures for CA acceptability;
- As a subject (including staff as subjects) - costs of PKCs and identifying CAs whose CP/CPS meet agency needs;
- Agency establishing itself as a CA/RA/AA.

Subjects (or their employers) usually have to buy their PKC, therefore agencies should avoid requiring specific certificates, except for attributes. The goal is that subjects, whether individuals or businesses, should need as few PKC as possible with maximum use from each.

Agencies should not require PKC with unnecessarily onerous proof of identity (or attribute). The strength of proof should be adequate for the purpose of the signature and the agency's risk management.

When agencies decide that they need to act as a CA, the technical operations should be outsourced rather than created within agencies.

When national standards and a CA certification regime become available agencies should use services from certified CAs. GATEKEEPER accredited suppliers should be used in the interim. If, for exceptional reasons, an agency fully establishes its own CA whose certificates are used outside the agency then such a CA must be certified under GATEKEEPER or national arrangements when these become available.

As relying parties, agencies should develop and maintain lists of CAs and PKC types that are acceptable for their purposes, taking particular care with CAs that are not independently certified by an independent external party/accredited.

Glossary

Asymmetric Cryptography

A type of cryptography using a pair of keys, where the same key cannot decrypt the information that it encrypted. Also called Public Key Cryptography. Uses Public and Private Keys.

Attribute Authority

A trusted organisation that creates and issues Attribute Certificates. May be the custodian of the attribute information (eg, a professional association) and/or a CA and/or RA.

Attribute Certificate

A certificate issued by an Attribute Authority that asserts that the subject has a particular privilege.

Authentication

Assurance of the identity of a person, system or organisation sufficient for a purpose.

Biometrics

An identity checking technique. Uses algorithmically created 'maps' of a person's physical characteristics (eg, voice, retina, face, finger whorls, hand geometry, written signature) that are stored and compared with maps re-created when invoked by a security system.

Certification Authority (CA)

A trusted organisation that issues PKC and associated private keys. May also undertake the role of Registration Authority.

Certification Policy

The statement by a CA setting out the purposes and conditions of the services supported by a particular type of PKC.

Certification Practice Statement

The statement of the practices (processes, procedures, etc) used by a CA to provide the services of a particular type of PKC.

Certificate Revocation List

A list maintained by a CA (or Attribute Authority) of all PKC (or Attribute Certificates) that have been cancelled before their stated validity expired.

Confidentiality

Measures taken to protect a document so that it can only be read by approved people or systems.

Cryptography

The mathematical science of deliberately scrambling and unscrambling information.

Digital Certificate

See PKC.

Decrypt

Mathematical techniques to unscramble encrypted information.

Digital Signature

Data unforgettably bound to a digital document that identifies the signatory and prevents undetectable changes to the document.

Document

A digital data file recorded on or in any medium or electronically (including optically) transmitted object. The data may be presented as information to any of a person's senses, most usually sight and/or hearing.

Electronic Signature

Any means of applying any form of signature to an item in digital form. A Digital Signature is one type of Electronic Signature.

Encrypt

Mathematical techniques to reversibly scramble information.

Government Public Key Authority (GPKA)

A Commonwealth body that operates its own accreditation process that qualifies highly trustworthy CAs. See Project Gatekeeper.

Hash

An algorithmic method to calculate a 'value', sometimes called the 'digest', of a document in digital form.

Identity Certificate

Synonymous with Digital Certificate.

Integrity

Measures taken to protect a document against unapproved modification.

Key

Any number used with an algorithm to Encrypt or Decrypt information.

Key Certificate

A type of certificate used in the distribution of a key for symmetric encryption.

Private Key

The Key in Asymmetric Cryptography that is kept private, normally to a single entity. For Digital Signatures it may be called the signature key.

Project GATEKEEPER

A Commonwealth project to create the GPKA and qualify highly trustworthy CAs.

Public Key

The Key in Asymmetric Cryptography that is widely distributed. For Digital Signatures it may be called the verification key.

Public Key Authentication

See PKC.

Public Key Certificate (PKC)

A data file issued by a CA to an entity that acquires a Digital Signature service. Includes information identifying the Subject, issuing CA, and period of validity, provides the subject's Public Key and is digitally signed by the CA. A CA may offer different types of PKC suitable for different purposes.

Public Key Cryptography

See Asymmetric Cryptography

Public Key Infrastructure

The policies, legislation, facilities and relationships that create a system of trustworthy CAs.

Registration Authority (RA)

An organisation that confirms the claimed identity of applicants for Digital Signature services.

Relying Party

An entity that receives a digitally signed item.

Subject

The entity that has Digital Signature services in their name and is issued with the PKC and Private Key.

Symmetric Cryptography

A type of cryptography where the same key is used to both encrypt and decrypt information. Also called Secret Key Cryptography. Typically used to encrypt complete documents for confidentiality reasons.

Trusted Authority

A body independent of subjects and relying parties that provides authentication services. Trustworthiness may be engendered by being part of an authentication framework and/or by independent assurance of operating practices.

X.509

The International Telecommunication Union (ITU-T) recommendation for an Authentication Framework. It provides the internationally agreed protocols and definitions for the objects and their attributes in a PKC. Identical with ISO/IEC 9594-