Evidential weight and legal admissibility of linking electronic identity to information
Evidential weight and legal admissibility of linking electronic identity to information

Code of practice for the implementation of BS 10008

*Peter Howes and Alan Shipman*
Contents

Foreword vii
Acknowledgements viii
Introduction ix
General xiii

1 Context of the organization 1
  1.1 General 1
  1.2 Issues 1
  1.3 Requirements 4
  1.4 Boundaries and applicability 5

2 Leadership 6
  2.1 Leadership and commitment 6
  2.2 Policy statements 6

3 Planning 16
  3.1 Actions to address risks and opportunities 16
  3.2 Objectives and achievements 17

4 Support 19
  4.1 Resources 19
  4.2 Competence 19
  4.3 Awareness 19
  4.4 Reporting and communications 19
  4.5 Documentation and records 20

5 Operation 29
  5.1 Management overview 29
  5.2 Technology considerations 29
  5.3 Keys and certificates 31
  5.4 Copyright issues 38
  5.5 Issuing authority 41
  5.6 Applying information attributes 42
  5.7 Applying and checking authorization 42
  5.8 Biometrics 43
  5.9 Encryption 45
  5.10 Compound documents 46
  5.11 Version control 46
  5.12 Migration 47
  5.13 Business continuity planning 47
  5.14 System maintenance 48
  5.15 Trusted third parties (TTPs) 48
  5.16 Time considerations 55

6 Performance evaluation 57
  6.1 Monitoring, measurement, analysis and evaluation 57
  6.2 Internal audit 57
  6.3 Audit planning 57
  6.4 Audit procedures 58
  6.5 Selection of auditors 59
  6.6 Management reviews 59
  6.7 Demonstrating compliance 60
# 7 Improvement

## 7.1 General

## 7.2 Preventive and corrective actions

## 7.3 Continual improvement

### Annex A Example electronic identity management policy statement

### Annex B References
Foreword

_Evidential weight and legal admissibility of linking electronic identity to information – Code of practice for the implementation of BS 10008_ (referred to in this document as ‘the Code’) is primarily concerned with the authenticity, integrity and availability of electronic identity, to the demonstrable levels of certainty required by an organization. It is particularly applicable where electronic identity attached to specific documents or other information may be used as evidence in disputes inside and outside the legal system.

This is the fifth edition of the Code, which was first published by BSI in 1998, as PD 5000. This edition is an editorial revision of the fourth edition (2008). It is technically similar, but has been restructured in recognition of the publication of BS 10008:2014, _Evidential weight and legal admissibility of electronic information — Specification_ and can be considered to be a guide to the implementation of the British Standard in relation to linking electronic identity to information.

Users of all previous editions should consider the advantages of assessing their information management systems in light of this new edition, and amend their systems and/or documentation where appropriate.

This publication is the third part of BIP 0008, which is made up of the following:

- BIP 0008-1 (2014), _Evidential weight and legal admissibility of information stored electronically — Code of practice for the implementation of BS 10008_; and
- BIP 0008-2 (2014), _Evidential weight and legal admissibility of information transferred electronically — Code of practice for the implementation of BS 10008_

The Code is published by BSI in recognition of the large number of implementations of electronic information management systems, and of the continuing uncertainty about the legal acceptability of an electronic identity linked to electronic information. It provides good practice guidance for the use of electronic identity management systems.
Acknowledgements

The Editors would especially like to thank the BSI Legal Admissibility Editorial Board and Panel, EOI Ltd and the members of technical committees IDT/1, Document management applications and IDT/1/-/5/, Revisions of BS 10008 for their business foresight in the development of this code of practice.

In particular, we would like to thank Jennifer Carruth from BSI for her excellent advice and copy-editing skills in developing BS 10008:2014.

Peter Howes
Alan Shipman
(Editors)

Group 5 Training Limited

The first edition of PD 5000, published in 1998, was sponsored by Group 5, in association with the Electronic Original Initiative.

BSI would like to thank the following people who reviewed the fifth edition of this book:

John Avallanet, Managing Director & Principal, Cerulean Associates LLC
Diane Shillito, Quality Systems Manager, CDS
Neil Maude, General Manager, Arena Group
Elisabeth Belisle, Managing Director, Scandox
Introduction

Electronic identity

The implementation and use of electronic information management systems and electronic communications systems provide significant benefits to many organizations. The traditional processes of associating identity with information to attest origin, authority or copyright ownership are, however, no longer sufficient and the process of 'signing', in ink, a paper document to confirm who produced, approved or authorized it may no longer be practically achievable or efficient. Methods for providing an equivalent to these identity marks need to be provided by such systems. The Code details operational procedures and technology requirements for these equivalent methods.

Many techniques are available to represent the intent or consent of an individual expressed in an electronic document or electronic transaction and to show that the electronic document or electronic transaction was actually created or approved by that particular individual, that is, the electronic equivalent of a handwritten signature.

Where copyright ownership can be associated with electronic information, additional evidence is available with regard to the identity of the information owner. Additionally, where electronic information has been encrypted, there may be additional evidence of the information owner.

INFORMATION – Identity theft: The problem

According to Action Fraud, the UK’s national fraud and internet crime reporting centre, identity theft is when personal details are stolen and identity fraud is the use of that stolen identity in criminal activity to obtain goods or services by deception.

Fraudsters can use identity details to:

- open bank accounts;
- obtain credit cards, loans and state benefits;
- order goods in the targeted person’s name;
- take over the targeted person’s existing accounts;
- take out mobile phone contracts; and
- obtain genuine documents such as passports and driving licences in the targeted person’s name.

Stealing an individual’s identity details does not, on its own, constitute identity fraud. But using that identity for any of the above activities does.

http://www.actionfraud.police.uk/fraud_protection/identity_fraud

In the UK, CIFAS (the UK’s Fraud Prevention Service) reported that the fraudulent use of identity details is the biggest and most perturbing fraud threat.

50% of all frauds identified in the UK during 2012 related to the impersonation of an innocent victim or the use of a completely false identity. Furthermore, whilst the number of fraud cases identified rose by 5% between 2011 and 2012 the number of identity fraud cases identified rose by 9.1% in the same period.

http://www.cifas.org.uk/fraudtrendstwentytwelve
Identity theft is a worldwide issue. In December 2013 the Justice Department’s Bureau of Justice Statistics (BJS) announced that an estimated 16.6 million people, representing 7 percent of all persons age 16 or older in the United States, experienced at least one incident of identity theft in 2012. Identity theft victims reported a total of $24.7 billion in direct and indirect losses attributed to all incidents of identity theft experienced in 2012. It is important to realize that these losses exceeded the $14 billion victims lost from all other property crimes (burglary, motor vehicle theft, and theft) measured by the US National Crime Victimization Survey for the same period.

http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821

The Code details procedures for the use of certificates that identify individuals or organizations as electronic versions of the manual ‘signing’ of documents by these individuals or organizations. An independent verification of such a certificate may be required either at the time of a specific action or process (e.g. an electronic communication being sent or stored), or subsequently. This part of BIP 0008 defines procedures that should be implemented when using such a facility.

For the purposes of the Code, an organization able to verify such certificates and signatures is referred to as a ‘trusted third party’ (TTP). A TTP is an organization that will perform the verification of certificates used by an organization, or issued to a particular individual. The TTP may be the original issuer of the certificates. In some cases, however, an agent of the TTP may have been the certificate issuer.

The American Bar Association publication, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, states that a TTP ‘must have sufficient financial resources:

1. to maintain its operations in conformity with its duties, and
2. to be reasonably able to bear its risk of liability to subscribers and persons relying on certificates issued by the certification authority [TTP].’

This basic tenet should be ascertained by the user of the TTP, especially as it is placing reliance and trust in the TTP’s services.

This in turn leads to another important factor. The level of surety required for a particular certificate may vary depending upon the value of the information being signed. The user needs to ensure that the liability accepted by the TTP is appropriate for the specific information being signed.

**INFORMATION – tScheme**

People and organizations need to have trust in e-commerce. To this end, commercial security services, generally called ‘trust services’, are being introduced to help defend against fraud and loss of privacy. tScheme was created to facilitate confidence that these ‘Trust Service Providers’ (TSPs), will deliver the services they claim to offer honestly and expertly.

tScheme is an independent, non-profit making, industry-led UK body set up to approve these services and provide that confidence. Membership of tScheme is actively encouraged across all interested sectors of UK industry, and a broad range of organizations are already represented and contributing to its development.

As awareness of e-security grows, an increasing number of end users and relying parties are looking for extra assurance before committing to online transactions. In particular they will look for a web seal to show that a website operates to particular standards. In the same way, the tScheme Mark acts as a trust seal to show that the service provider is following best practice.

According to tScheme, ‘When a trust service carries the tScheme Mark, you can be confident that:
• the service has been thoroughly evaluated against rigorous criteria by independent experts;
• the service provider has agreed to keep to these criteria;
• the service provider subscribes to the tScheme Code of Conduct; and
• the service provider has agreed to act promptly and fairly to remedy faults.’

http://www.tscheme.org/

The Code details information that a user should check before using a TTP. It also details issues that a TTP should address.

A number of these areas will be relatively new to many organizations. Key and certificate issuing organizations and service providers, however, offer products and services that address these areas. Their guidance can be very useful, but, as with all service or product suppliers, the onus will rest with the user (organization or individual) rather than with the supplier.

Many service providers will include a certificate policy and a ‘certification practice statement’ (CPS) as part of their commitment to their users. These (and the supplier’s contract) need to be reviewed in detail against the organization’s requirements if such a supplier is used.

**Purpose of the Code**

The Code covers:

• sender and recipient identity verification;
• evidentially provable electronic signatures; and
• linking identity of copyright ownership to electronic information.

The Code also covers the application of technology to provide electronic message sender and recipient identity verification; this is the association of identity with a transferred document. This may be by the use of a digital signature; where the similar or associated cryptographic techniques are also used for confidentiality, this application is addressed in this part of BIP 0008.

The Code does not cover the application of identity and identity tokens for access to services. These logical and physical access control functions may well use techniques in common with those used in the Code. The fundamental question asked when an identity is attributed to an individual is ‘Are they really who they say they are?’ is a common issue that must be addressed.

The Code does not recommend specific technologies – it simply details required attributes, procedures and processes to be applied, together with the requirements for the audit of such systems.

**Management framework**

Chapters 1 to 7 of the Code are structured along the lines of the standardized structure of ISO Management System Standards, such that its implementation can be synchronised with other management systems such as BS ISO/IEC 27001:2013 Information technology — Security techniques — Information security management system — Requirements, where appropriate.
Seven chapters of BIP 0008-3

1. Context of the organization
   1.1 General
   1.2 Issues
   1.3 Requirements
   1.4 Boundaries and applicability

2. Leadership
   2.1 Leadership and commitment
   2.2 Policy statements

3. Planning
   3.1 Actions to address risks and opportunities
   3.2 Objectives and achievements

4. Support
   4.1 Resources
   4.2 Competence
   4.3 Awareness
   4.4 Reporting and communications
   4.5 Documentation and records

5. Operation
   5.1 Management overview
   5.2 Technology considerations
   5.3 Keys and certificates
   5.4 Copyright issues
   5.5 Issuing authority
   5.6 Applying Information attributes
   5.7 Applying and checking authorization
   5.8 Biometrics
   5.9 Encryption
   5.10 Compound documents
   5.11 Version control
   5.12 Migration
   5.13 Business continuity planning
   5.14 System maintenance
   5.15 Trusted third parties
   5.16 Time considerations

6. Performance evaluation
   6.1 Monitoring, measurement, analysis and evaluation
   6.2 Internal audit
   6.3 Audit planning
   6.4 Audit procedures
   6.5 Section of auditors
   6.6 Management reviews
   6.7 Demonstrating compliance

7. Improvement
   7.1 General
   7.2 Preventive and corrective actions
   7.3 Continual improvement
General

Scope
This part of the Code covers procedures and processes relevant to the following electronic information authentication principles:

- electronic identity verification – proving the genuineness of the individual/organization that produced, transferred and/or stored the electronic document;
- electronic signature – the application of the legal equivalent of a ‘pen and ink’ signature on a paper document;
- electronic copyright – the application of a copyright mark to an electronic information; and
- linking the electronic identity and/or electronic signature and/or electronic copyright to the particular electronic information (and preventing compromise to its integrity).

The identity of the originator or sender of electronic information may need to be demonstrated, particularly where problems of false identity have been detected, or are suspected. This requirement is particularly applicable where internet communications are involved. Typically, robust and trustworthy electronic verification of identity is applied using cryptographic techniques, by the issue and use of certificates involving Private and Public Key technologies.

Where electronic signatures are used, the Code provides guidelines for ensuring that such signatures will replace or enhance an existing written signature. Such signatures need to be selected and utilized without unexpected compromise to the parties involved in the exchange of signed information and its verification and validation. Electronic signatures will, in all cases, need to be supported by an electronic identity.

Where electronic copyright protection systems are used, the Code provides guidelines for their use. In the context of the Code, copyright does not include collection of licence fees, purely the protection and linking of copyright holding by an entity to a document.

INFORMATION – Digital rights management

Digital rights management (DRM) is an umbrella term for legally binding technical protection measures that allow owners of copyrighted digital content to control digital content after an ordinary contractless sale of the content.

DRM poses one of the greatest challenges for content communities in this digital age. Traditional rights management of physical material benefited from the material’s physicality as this provided some barriers to unauthorized exploitation of content. Today, however, we already see serious breaches of copyright law because of the ease with which digital files can be copied and transmitted.

First-generation DRM systems focused on security and encryption as a means of solving the issue of unauthorized copying; that is, lock the content and limit its distribution to only those who pay. A well understood example of this is the supply of a one-time key to complete installation of downloaded software and enforced web based registration to ensure the software is not repetitively installed in contravention of the licence.

This approach was substantially narrower than the broader capabilities of second-generation DRM systems. The second generation of DRM covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets, including management of rights holders’ relationships. Additionally, it is important to note that DRM is the ‘digital management of rights’ and not the ‘management of digital rights’. That is, DRM manages all rights, not only the rights applicable to permissions over digital content.
DRM systems restrict the use of digital files in order to protect the interests of copyright holders. DRM technologies can control file access (number of views and/or length of views), altering, sharing, copying, printing and saving. These technologies may be contained within the operating system or program software, or in the actual hardware of a device.

DRM systems take two approaches to securing content. The first is ‘containment’, an approach where the content is encrypted in a shell so that it can only be accessed by authorized users. The second is ‘marking’, the practice of placing a watermark, flag or XML tag (BS ISO/IEC 21000-5:2004, Information technology — Multimedia framework (MPEG-21) — Part 5: Rights Expression Language) on content as a signal to a device that the media is copy protected.¹

Information rights management (IRM), sometimes also called Enterprise Digital Rights Management, is a subset of DRM. IRM is used to protect sensitive information from unauthorized access typically in a business-to-business model (e.g. financial data, intellectual property,¹ executive communications). IRM allows for information (mostly in the form of documents and emails) to be ‘remote controlled’. This means that information and its control can now be separately created, viewed, edited and distributed.

Whilst not necessarily evidential weight and legal admissibility issues, and because similar cryptographic techniques are often used, the Code also provides guidance for provision of confidentiality issues, by ensuring that the information cannot be seen by unauthorized individuals. Confidentiality of information is typically handled by applying cryptographic encoding to the information, so that it can only be accessed by someone having the appropriate decoding processes and keys.

**COMMENT**

Email has become an essential business tool, but it must be used with care if the sender or recipient is to rely upon email in the event of a dispute. It is not technically difficult to make an email appear to come from someone other than the real sender. This ID ‘spoofing’ is used extensively by spammers to mask their identities.

Many secure email services use ‘Secure/Multipurpose Internet Mail Extensions’ (S/MIME), which provide a consistent way to send and receive secure MIME data. See the Internet Engineering Task Force’s (IETF’s) RFC 3851 (to be replaced by 5751). Based on the widely adopted internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications:

- authentication;
- message integrity and non-repudiation of origin (using digital signatures); and
- data confidentiality (using encryption).

A note of caution: to enable the internet mail infrastructure to route confidential messages that include S/MIME, there are parts of the message that cannot be encrypted, for instance, the recipient and sender identity details.

**Applicability**

This part of the Code is applicable to electronic identity management systems and can be applied to any form of electronic identity management system, irrespective of the technology used.

¹ www.ipo.gov.uk/types/copy.htm
The users

The Code is intended for:

- end user organizations that wish to ensure that electronic identity management systems may be used with confidence as evidence in any dispute, within or outside a court of law; and
- integrators and developers of electronic identity management systems that provide facilities to meet user requirements.

Objectives

The objectives of the Code are to:

- improve the reliability of, and confidence in, electronic information to which an electronic identity is applied;
- maximize the evidential weight that a court or other body may assign to presented information;
- provide confidence in inter-organization trading; and
- provide confidence to external inspectors (for example, regulators and auditors) and stakeholders that the organization’s electronic identity practices are robust and reliable.

The Code may be used as a common reference standard for business activities within and between organizations and for subcontracting or procurement of IT services or products.

Compliance

Each chapter of the Code contains a general description of the issues being addressed, followed by a list of ‘key issues’. These key issues indicate the critical compliance points that need to be taken into consideration, and acted upon where appropriate, before compliance with the recommendations of the Code can be claimed. Compliance is claimed on a voluntary basis, by self-certification.

A compliance workbook (BIP 0009 (2014)), Evidential weight and legal admissibility of electronic information — Compliance workbook for use with BS 10008) has been published to enable an assessment of compliance with BS 10008 to be completed. Where critical compliance points from the Code are not specifically included in the British Standard, these points are included as an optional component in the compliance workbook.

Typical compliance statements are shown in 6.7.2. See also 6.7 for information on compliance audits.

Key requirements

Included in the controls for the Code are a number of underlying criteria that, when complied with, provide assurances that electronic identity management systems have been used in a controlled and understandable manner. As such, they are applicable to both the sender and the recipient of electronic communications.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proof of identity</td>
<td>Ensuring that keys and certificates are added by the appropriate individual and/or organization</td>
</tr>
<tr>
<td>Security of keys and certificates</td>
<td>Ensuring that keys are not compromised prior to and after they have been added to electronic information</td>
</tr>
<tr>
<td>Reliable copyright protection systems</td>
<td>Ensuring that copyright is not compromised</td>
</tr>
<tr>
<td>Date and time of attribution</td>
<td>Identifying the time of adding information attributes</td>
</tr>
<tr>
<td>User acceptance</td>
<td>Ensuring that authorized recipients can reliably interpret keys and certificates</td>
</tr>
</tbody>
</table>

Table 1 – Key requirements for maximizing the evidential weight of electronic identity management systems
1 Context of the organization

1.1 General

This section of the Code relates to Clause 4 of BS 10008, ‘Context of the organization’.

With the move from paper originals to electronic original documents, the use of the electronic equivalent of an ink signature becomes an important part of a document authorization process. A signature can also be used as a method for authenticating the contents of a document.

Technologies can be implemented that apply electronic signatures of various forms to electronic documents, with various degrees of confidence and integrity. Some systems also allow for the verification of an electronic signature by another individual or organization (a TTP).

As with many types of electronic system, however, simply implementing technology may not provide the weight of evidence necessary should an electronic identity be challenged. The implementation of appropriate policies and procedures is necessary in order to create secure, structured and auditable electronic identity management systems.

1.2 Issues

The organization needs to determine the external and internal issues that are relevant to its purpose and that may affect the authenticity and integrity of the information managed by the identity management systems.

The requirement to authenticate electronic information assets that have evidential significance to an organization may be vital to continued operations. Such authentication systems are becoming more widespread, and various features have been established by organizations involved with these systems. Authentication in the Code deals with proof of identity in relation to document signatories, and to copyright issues.

INFORMATION – Electronic and digital signatures

The term electronic signature and digital signature are often used interchangeably – they are not the same and the law, in most jurisdictions, goes to some length to clearly distinguish between them.

Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature.

There are many forms of electronic signature, many of which are not particularly resistant to fraud (but it must be remembered that fraud is also prevalent with handwritten ‘wet’ signatures).

Electronic signatures have many of the same problems as handwritten signatures but also have some others to consider.

Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

The digital signature uses a pair of cryptographic keys; one of these keys is Private and the other is Public. The Public Key is shared but the Private Key must be retained securely.
If someone else has access to an individual's Private Key then they can fraudulently digitally sign for that individual as an imposter. This is why security of the Private Key is critical to the robustness and trustworthiness of something digitally signed.

The two important attributes of digitally signed information are:

• the signer is the person with the Private Key; and
• what was signed has not been changed since the act of signing.

It is essential at the planning stage to consult with appropriate third parties that will need to use or inspect the results from authentication systems as detailed in the Code. Examples of such third parties are:

• receiving parties;
• auditors;
• legal experts; and
• technical and operational staff.

The requirement to verify digital or electronic signatures or other identification systems of electronic information by third parties, with full legal significance, is far-reaching. Such verification systems based on digital certificates are becoming more frequently required, as an independent check on electronic information integrity, origination, authority and authenticity.

Similarly, the successful use of copyright protection systems may be critical to the success of an organization.

Thus, when designing and implementing procedures for the verification of such systems in the event of a challenge from another organization, it is essential to consult with organizations that provide independent verification services (TTPs).

Different organizations may not be using the same TTP. Where this situation occurs, the procedures for the various TTPs may be different, as might the services offered, the rigour of checks performed and liabilities accepted. Strict control will be needed under these circumstances.

The user of a specific TTP needs to be aware of the ‘network of trust’ that their TTP is a part of, and should ensure that its liability for certificate verification is handled by its TTP (and not ‘passed on’ along the chain to a less trustworthy organization).

**INFORMATION – Encryption keys**

Software, usually on a user's computer, generates the pair of encryption keys that will be used in secured applications – a Public and a Private Key.

The Private Key is never distributed or revealed; conversely, the Public Key is freely distributed to any party that negotiates a secure transfer.

During the registration or enrolment process, the user's Public Key is sent in a certificate request to the certification authority (CA) or its authorized agent, a registration authority.

When the CA approves the request, it generates the user's digital certificate. The user’s certificate will have been digitally signed by the CA. After the user receives his or her certificate and installs it on the computer, he or she can participate in the secured application.
The user’s digital certificate (an X.509 certificate) contains the user’s Public Key and has been digitally signed by the CA after checking that the user really is who they purport to be (this may be to different levels of confidence depending on how the checks are conducted). The digital certificate is then used either for encryption or digitally signing (frequently there will be two sets of keys and two certificates; one for encryption and a separate one for digital signing). The digital certificate, containing the user’s Public Key, is used by someone wishing to encrypt data for that user; the user decrypts that data using their Private Key. For digital signing, the user’s Private Key is used and the Public Key (in the certificate) is then able to confirm the integrity of the signed content and that it was signed by the user (whose identity was confirmed by the CA before they signed the user’s certificate.

**INFORMATION – Hierarchy of trust**

There is a concept of hierarchy of trust; this is simply that there must be a CA that everyone agrees is trustworthy. This ultimate authority is called the root CA. The root authority can then certify other CAs below it, which can then certify CAs below them, etc. This is illustrated in the diagram overleaf.

When a certificate is received that has been issued by a first or second level CA, the user can verify that the CA that signed the certificate has been certified by a CA at the level above it and, in turn, that CA has been certified by the one above that, and so on until a chain of trust exists between the lower level CA (or a user certificate) and the root CA. For example, in the diagram, it can be verified that CA No. 3 was certified by CA No. 1, and that CA No. 1 was certified by the Root CA.

When a certificate from a lower level CA is passed along with an encrypted message, all of the certificates in its chain of trust up to the root should be passed along with it.
The organization, therefore, needs to ensure that the agreements between the members of the
network of TTPs are adequate to deliver the required verification service and that the fiscal guarantees
in the event of failure are sufficient to meet its requirements.

1.3 Requirements
When establishing or reviewing the systems and/or processes that manage the evidential weight of the
identity management system, the organization needs to determine:

a) stakeholders that are relevant to the authenticity and integrity of information;
b) the requirements of these stakeholders relevant to that information; and

c) the requirements for information stewardship within the organization.

NOTE: The requirements of stakeholders may include legal and regulatory requirements and contractual obligations.

Typical stakeholders may include:

- owners, managers and staff of the organization;
- third parties with contracts or similar agreements with the organization;
- clients and customers in receipt of services provided by the organization;
- the public where public services are involved;
- regulatory bodies;
- government bodies;
- external audit bodies; and
- legal advisers.

The requirements of each stakeholder need to be taken into consideration when producing policy
statements (see 2.2).

Information stewardship should be managed by the identification of information asset owners (IAO’s)
who will typically be those responsible for the processes that generate the information asset in
question.
1.4 Boundaries and applicability

The organization needs to determine the boundaries and applicability of the authenticity and integrity of the information managed by the identity management systems in order to establish its scope.

When determining this scope, the organization needs to consider:

a) the external and internal issues referred to in 1.2;
b) the requirements referred to in 1.3; and
c) interfaces and dependencies between activities performed by the organization and those that are performed by other organizations.

The scope needs to be available as part of the policy document.