Evidential weight and legal admissibility of linking electronic identity to information

Code of practice for the implementation of BS 10008

Fifth Edition

Peter Howes and Alan Shipman

bsi.

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

bsi.

First published in the UK in 1998
Second edition 2002
Third edition 2005
Fourth edition 2008
Fifth edition 2014

by
BSI Standards Limited
389 Chiswick High Road
London W4 4AL

Typeset in Frutiger by Letterpart Limited, letterpart.com

Printed in Great Britain by Berforts Group, www.berforts.co.uk

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 978 0 580 85678 5

Contents

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 and committees IDT/1, Document management applications and IDT/1/-/5, Revisions of BS 10008 for their contribution to the current and previous editions of this publication, in particular for their business foresight and tireless reading of the manuscript. Their suggestions for improvements added value to the final publications.

The members of IDT/1 are Martin Bailey, Ian Curington, Aandi Inston, Marc Fresko, Peter Howes, Philip Jones, Andrew Kenny, Bill Mayon-White, Roger S Poole, Nick Pope, Ian Walden, Leonie Watson, Andrew Pibworth, Neil Pitman, Alan Shipman and Tom Wilson.

The members of IDT/1/-/5 are Elisabeth Belisle, Bernie Dyer, Peter Howes, Richard Jeffrey-Cook, Bill Mayon-White, Roger S Poole, Alan Shipman, Rod Stone and Tom Wilson.

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.

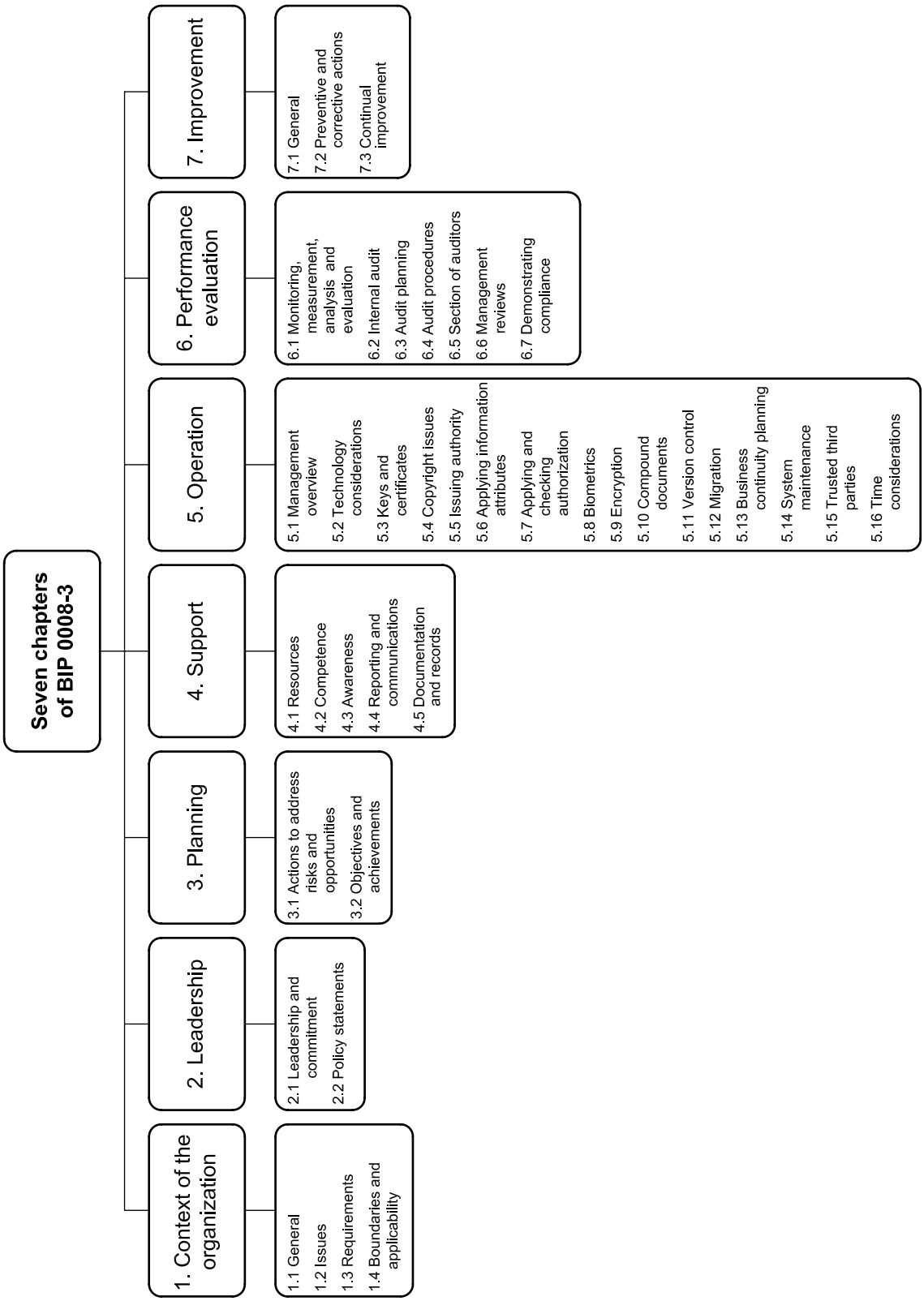
The Code also covers the application of technology to provide electronic message sender and recipient identity verification; this is the association of identity with a transferred document. This may be by the use of a digital signature; where the similar or associated cryptographic techniques are also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

Topic	Requirement
Proof of identity	Ensuring that keys and certificates are added by the appropriate individual and/or organization
Security of keys and certificates	Ensuring that keys are not compromised prior to and after they have been added to electronic information
Reliable copyright protection systems	Ensuring that copyright is not compromised
Date and time of attribution	Identifying the time of adding information attributes
User acceptance	Ensuring that authorized recipients can reliably interpret keys and certificates

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

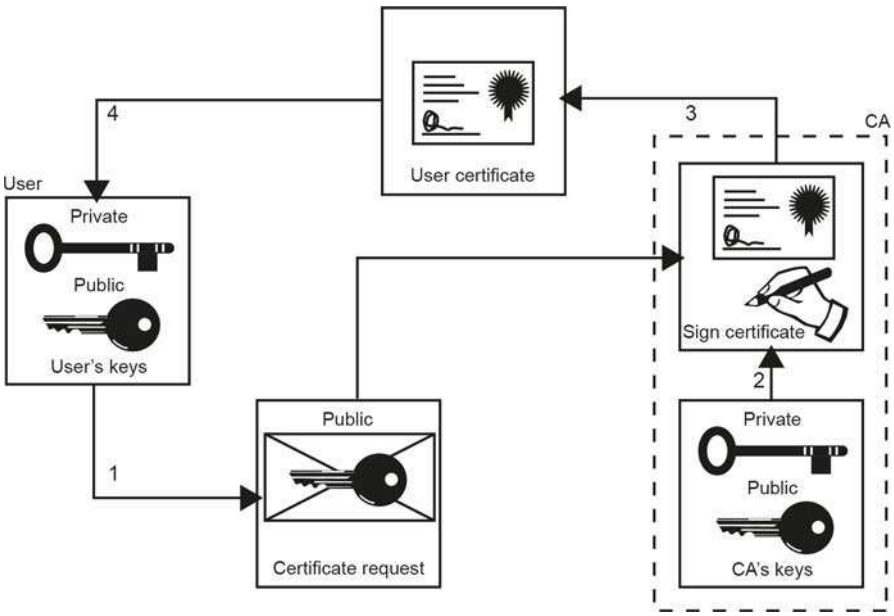
Software, usually on a user's computer, generates the pair of encryption keys that will be used in secured applications – a Public and a Private Key.

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.

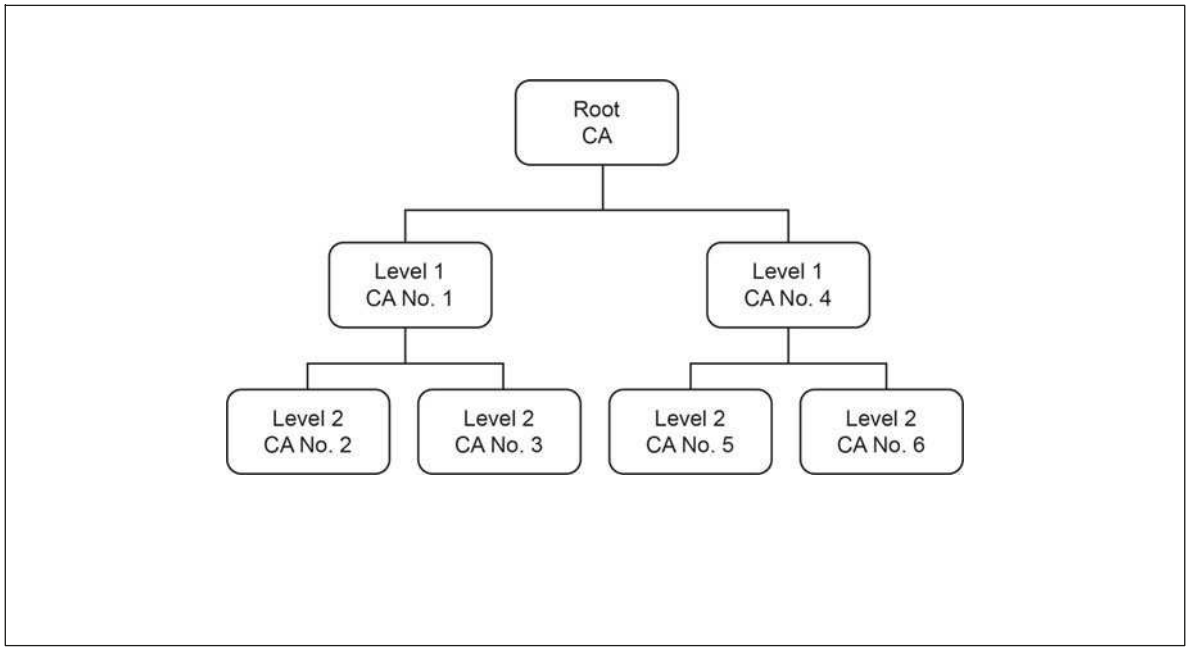


INFORMATION – Hierarchy of trust

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.

2 Leadership

2.1 Leadership and commitment

This section of the Code relates to Clause 5 of BS 10008, 'Leadership'.

Top management needs to demonstrate leadership and commitment with respect to the management of the authenticity and integrity of information managed by the identity management system by:

a) ensuring that the identity management policies and objectives are established and are compatible with the strategic direction of the organization;
b) ensuring the integration of the identity management system requirements into the organization's processes;
c) ensuring that the resources needed for the identity management system are available;
d) communicating the importance of effective identity management and of conforming to the identity management system requirements;
e) ensuring that the identity management system achieves its intended outcome(s);
f) directing and supporting persons to contribute to the effectiveness of the identity management system;
g) promoting continual improvement; and
h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

2.2 Policy statements

2.2.1 General

Different types of document may be electronically signed by an organization or by a worker on behalf of an organization. The receiving organization needs to be able to verify these signatures. To enable the implementation of such systems, the organization needs a policy statement that can be used to guide implementers, and to demonstrate to other parties that systems used were in line with policy.

Where an organization uses TTPs such as CAs, the policy statement should include the policy for their use.

2.2.2 Electronic identity policy statement

2.2.2.1 Structure

To implement the Code, the policy statement produced in compliance with BIP 0008-1 should be extended to include policy on electronic identity management.

The policy statement should be approved by the top management of the organization and reviewed for relevance and content at regular intervals. The frequency of review should be appropriate to the application. This period will typically be the same as the normal procedural audit cycle within the organization, for example annual or in the event of major changes to the system.

There will frequently be more than one type of electronic identity management system in use within an organization. The identity requirements for each document type need to be reviewed, based on timeliness and service levels. Cost may also be a consideration.

In order to align electronic identity requirements with specific electronic documents, a document 'type' designation should be allocated. These types may be described by application (e.g. financial reports or stock lists) or by information content (e.g. an invoice or an order).

The policy statement should set out guidelines for the appropriate application of an electronic identity for each document type. This statement should include the organizational requirements for identity, authority and copyright protection.

The policy statement should document the level and rigour of protection required, detailing the requirements for each document type.

Where there is a requirement, the policy statement should describe the degree of security required, for example some documents are not as significant as others and proof of the signatory's identity is of less importance – for instance, an internal memo as opposed to a contractual commitment.

The underlying issue with these items is: who will be required to understand the significance of an electronic identity attached to a document? If it is always someone within the same organization, it is significantly less complex than between organizations because the organization can set its own rules. For all inter-organizational documents controlled with electronic signatures or copyright protection, it is imperative that the recipient organization is capable of understanding the significance of what is communicated to it, recognizing, implementing and utilizing the relevant controls.

Annex A includes an example electronic identity management policy statement, which may be used during the drafting of an organization's policy statement. It contains some 'typical' statements that may be appropriate in many policy statements.

EXAMPLE

For some electronic documents, it is important that the identity of the signatory is reliable and can be trusted. For other electronic documents, the actual identity of the author may not be important.

For example, an electronic order for goods of high value may need to be signed by an authorized member of staff. The receiving organization would have a list of approved signatories. The order would need to have a verifiable signature attached.

An order for a train ticket over the internet does not, however, need to be signed. The railway company is happy to receive the value of the ticket by the entry of validated credit card details. The identity of the traveller is not important to the transaction.

2.2.2.2 Content

The use of the term 'keys and certificates' is applied to any appropriate and acceptable cryptographic technology that can be used to verify:

- identity;
- electronic signatures;
- electronic copyright.

The same principles will need to be followed where biometric technologies are used.

INFORMATION – Biometrics

Biometrics are methods by which the identity of an individual can be confirmed. They are used by comparing a newly captured biometric attribute with the biometric that was captured during a controlled registration process, when the link between the biometric and the physical identity could be verified. The attributes are gathered by measuring a person's appropriate physiological or behavioural features.

The term 'biometric' is derived from the ancient Greek words 'bios' for life and 'metron' for measure.

In IT, biometrics usually refers to the technologies for measuring and analysing human physiological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, especially for authentication purposes. Examples of behavioural characteristics that can be measured include signature recognition, gait recognition and typing recognition.

The policy statement should include the organization's policy (for each document type) on:

- applicable protection techniques that may be used;
- responsibilities for the control and management of these techniques; and
- the control and management of keys and certificates (if used).

Where third parties are involved, the responsibilities and liabilities of those third parties should be clearly identified.

The policy statement should also include the organization's policy on:

- the verification of the validity of certificates and signatures;
- reacting to challenges to certificates and signatures;
- where appropriate, the selection criteria for TTPs;
- arbitration routes as an independent mechanism for enabling the resolution of disputed challenges; and
- retention periods (and other information) for documents created during the verification process, including audit trail data.

KEY ISSUES

> Develop an electronic identity management policy statement and have it approved by top management.
> Ensure it is reviewed at regular intervals, as appropriate to the application.

2.2.2.3 Consultations

In some jurisdictions, restrictions apply as to the types and complexity of cryptographic keys that may be used for encryption and electronic signature purposes. These restrictions should be evaluated and complied with as appropriate.

In some jurisdictions, encryption may not be allowed, or may only be allowed to a certain level. Electronic signatures may, however, be allowed. In this event, it is important to verify that the techniques employed can only be used for the provision of electronic signatures.

If there is doubt about local legislation, the use of a TTP should be considered, particularly where it is able to meet local legislative practices.

A TTP needs to be able to demonstrate its awareness of the value of the service that it provides, which needs to be executed under its responsibilities under the duty of care principle.

To fulfil this objective, the organization should ensure that the TTP can demonstrate its awareness of:

- legislation and regulatory bodies pertinent to the TTP and the organization's industry;
- legislation pertinent to countries (or other geographical areas) where its services are delivered;
- the accountability and responsibility requirements for activities involving verification services at all levels; and
- developments, by keeping in contact with the appropriate bodies and organizations.

KEY ISSUES

> Where encryption is used, any local legal restrictions should be identified and complied with.
> The use of local TTPs may assist in this process.

2.2.2.4 Roles and responsibilities

The policy statement should include a statement, for each document type, of the individual responsible for the management of the electronic identity management systems.

The policy statement should include a statement of the responsibility for the issue of verification requests. Such authority may be vested in an individual, or a group of individuals, specified by name or by role. The organization should ensure that the TTP is aware of these responsibilities, and only accepts verification requests from authorized individuals.

KEY ISSUES

> Individual responsibilities for the electronic identity management systems should be specified.
> Responsibilities for the issue of verification requests should be specified.

2.2.2.5 Assignment of rights

The policy statement should include a statement, for each document type being stored, of how the assignment of rights to a document is vested in specific persons or is granted to such.

KEY ISSUE

> Individual responsibilities for the assignment of document rights should be specified.

2.2.2.6 Procedures

The policy statement should provide guidelines on the requirement for appropriate procedures to be followed when electronic identity management is being undertaken. Details of these procedures can be found in Chapter 5. These procedures may need to link to the organization's information security policy as detailed in 2.2.3.

KEY ISSUE

> The policy document should give guidelines on the procedures necessary to use the organization's electronic identity management systems.

2.2.3 Information security management

2.2.3.1 Management overview

The organization should be aware of the value of its electronic identity management systems, and execute its responsibilities to those systems under the duty of care principle.

Whilst the organization may utilize one or several trusted third-party service providers, the organization cannot outsource its duty of care responsibilities.

To fulfil its duty of care obligations, the organization should:

- be aware of and demonstrably comply with legislation and regulatory bodies pertinent to its industry;
- be aware of and demonstrably comply with legislation and regulatory bodies pertinent to its country (or other relevant geographical area) of origin, routing and/or receipt of electronic identity document attributes;
- establish a chain of accountability and assign responsibility for all relevant activities; and
- keep abreast of developments by keeping in contact with the appropriate bodies and organizations.

2.2.3.2 Security management guidance

Publications are available that provide advice in devising comprehensive sets of information security guidelines to meet the organization's needs. These may be included in the organization's review process. For some applications, the adoption of externally accredited security schemes as additional confirmation of compliance to their security policy may be appropriate.

There are a number of national and international standards that, if implemented, should support the organization's demonstration of duty of care. Standards that cover information security and service quality issues are particularly appropriate.

COMMENT

The internationally accepted information security management standards are:

BS ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*;

BS ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*.

Information is the lifeblood of all organizations and can exist in many forms. It can be stored electronically and transmitted by mail or by electronic means. In the competitive business environment, such information is constantly under threat from many sources. These can be internal, external, accidental or malicious.

These information security standards address these issues and have thus been implemented in many major organizations. They are referenced in many places and are becoming the common benchmark against which information security is measured.

Within the UK, there is a formal certification scheme against the requirements of BS ISO/IEC 27001. A number of UK and overseas organizations have seen the benefit of compliance, particularly where they offer IT services to other organizations. Other organizations have used the two documents to assess their information security management systems, as part of their risk assessment processes.

It is important that any decisions made concerning certification or compliance with the standards are recorded by the organization.

KEY ISSUE

> Where an appropriate national or international standard is implemented, electronic identity management systems should be included within the scope of compliance with the standard.

2.2.3.3 Scope

To fulfil the duty of care objective, the organization needs to action the following.

Topic	Action	Section
Information security policy	Implement an information security policy	2.2.3.4
Risk assessment	Carry out a risk assessment and implement appropriate recommendations	3.1.2
Information security infrastructure	Develop, implement and test an information security management system	2.2.3.6
Business continuity planning	Develop, implement and test a business continuity plan	5.13
Choosing a TTP	Choose an appropriate third party	2.2.4
Contracts	Ensure an appropriate contract is in place with third parties	2.2.5

Table 2 – Actions required to fulfil the care of duty objective

2.2.3.4 Information security policy

All electronic identity management systems are vulnerable to compromise or change, whether accidental or malicious. To protect these systems, appropriate security measures need to be implemented to reduce the risk of such a compromise or change and thus a successful challenge to their effectiveness.

Security measures need to be implemented which ensure that the application of electronic identity is controlled, reliable and auditable.

Similarly, security measures need to be implemented to protect the information that is being secured using keys and/or certificates. Such security measures are important, both for the organization and for a TTP.

Information security, whether in the area of confidentiality, integrity or availability (CIA), is not simply a constraint to be placed upon computer systems. Security and access to the physical environment, for example buildings and networks, and the implementation of policies and procedures by all staff are key elements.

The organization should adopt an information security policy in relation to electronic identity management systems. Where an information security policy exists for other processes (for example, storage), the use of electronic identity and authentication techniques should be incorporated within its scope.

The organization should confirm that any TTPs that it uses have adopted their own information security policies.

Where document verification keys, certificates and other information are archived by a TTP, they should be stored in compliance with that TTP's information security policy.

COMMENT

Compliance with the recommendations of BS ISO/IEC 27002 is widely recommended; certification against BS ISO/IEC 27001 is a way of demonstrating to other organizations that the above requirements are being met.

Such independent accreditation is commonly regarded by TTPs as a means of proving their credentials to their customers. Therefore, the tScheme publication, *Guidance for Assessments*, references compliance with information security management and formal accreditation against BS ISO/IEC 17799 (now BS ISO/IEC 27001). This certification is not mandated; it is a business decision of the TTP.

The tScheme *Guidance for Assessments* (tSi0250) can be found in the tScheme Library: http://www.tscheme.org/library/index.html#guidelines

The information security policy should contain (for the electronic identity and authentication techniques), as a minimum:

- a scope;
- management objectives regarding the use of electronic identity and authentication techniques;
- management objectives regarding information security for the use of keys and certificates;
- specific policy statements;
- the allocation of information security responsibilities;
- a definition of electronic identity and authentication techniques and responsibilities;
- a definition of responsibilities for keys and certificates;
- training in, and awareness of, the use of electronic identity and authentication techniques;
- key and certificate training and awareness;
- a policy for dealing with potential or actual compromises of electronic identity and authentication techniques;
- a policy for dealing with potential or actual compromises of keys and certificates;
- a policy regarding compliance with appropriate standards; and
- an approval and review process.

Different types of information may require different electronic identity and authentication techniques. These should be identified in the policy statement (see 2.2.3.4).

Where security requirements vary for different document types, the information security policy should identify appropriate needs. These measures need to be considered in the light of utilizing a TTP.

The organization should ensure that its own information security requirements are met by the chosen TTP. The TTP may not wish to publicize actual security procedures, but needs to be able to demonstrate to the organization that it is compliant with this part of the Code.

Different types of keys and certificates may need different security measures. These need to be identified in the information security policy.

KEY ISSUES

> Develop, authorize and implement an information security policy.
> Ensure that the policy's scope includes the electronic identity management systems.

2.2.3.5 Risk assessment

Information security measures are often applied piecemeal, reacting to security incidents or to available computer software tools. This type of approach can fail to recognize the value of the information asset and the risks to the organization from security compromise of electronic identity and authentication techniques. This may leave gaps in security, which may only be filled at some later date, after a security breach.

A more structured approach is to review the information assets and assign risk factors (based on asset value, system vulnerability and likelihood of attack). The information security policy can then be produced and approved against the value model.

Existing security measures should then be reviewed for effectiveness. Factors such as the balance between the cost of implementation and the security achieved should be taken into consideration during the review process.

Where different types of electronic identity and authentication techniques can be used, their individual impact on the risk analysis results should be reviewed.

Recommendations identified by the risk analysis should be implemented.

The organization should also undertake a risk assessment of the services provided by TTPs.

BS ISO 31000:2009, *Risk management — Principles and guidelines* provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. It can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

KEY ISSUE

> Use risk assessment techniques to ensure that existing information security measures are appropriate, or to identify any measures that need to be taken to improve security.

2.2.3.6 Information security infrastructure

In order to control and manage information security issues with keys and certificates for electronic identity and authentication, an infrastructure needs to be implemented, including relevant systems within its scope.

A management infrastructure, or framework, as defined in BIP 0008-1 should include within its scope electronic identity and authentication techniques.

KEY ISSUE

> Plan and implement an information security framework.

2.2.4 Choosing a TTP

An organization using, and hence depending upon, a TTP for the independent verification of digital signatures and/or copyright protection systems needs to understand and accept the full details of its services.

The organization should review the procedures and processes implemented by a potential TTP, using the recommendations of all three parts of the Code as a benchmark for suitability. However, compliance with these recommendations may not need to be a necessary component of a contract between the organization and a TTP (see 2.2.5).

Trusted third parties should be able to demonstrate that they act in an appropriate manner bearing in mind the location (e.g. country) and legal system in which they and/or their clients (and/or the challenger) operate.

During the initial discussions prior to contract agreement, the TTP should disclose any duty or obligation it is under to make information relating to its services available to any other party, including government and regulatory agencies.

The TTP should be able to demonstrate that procedures for different organizations are applied as appropriate, and that any information, keys and certificates it holds are segregated from those of other organizations for which it provides services.

A TTP will normally have amongst its standard documentation set two key formal documents: a certificate policy and a CPS. Both form part of its obligations to the customer, the user. The user should not assume that either the offer detailed in the certificate policy or the CPS or other standard documents meets its requirements or that the CA will perform to the levels stated in them or its contracts. The user should confirm that its needs are reflected and that suitable performance criteria are present, especially in business-to-business situations.

The CPS, and all other documents concerning the agreement with the TTP, should be treated as business critical documents of the organization and be retained in accordance with BIP 0008-1.

KEY ISSUE

> Trusted third parties should be chosen with care, to ensure that their services are appropriate to the requirements of the organization.

2.2.5 Contracts

Where a TTP is used as part of the process for electronic identity management, an appropriately worded contract should be agreed between the organization and the TTP. This contract should include details of the services that are to be used.

The contract should be retained securely by the organization in compliance with BIP 0008-1. Whilst it is an advantage for the contract to include the requirement for compliance by the TTP with all relevant recommendations of the Code, it is not essential. Where the contract does not specify compliance with the Code, service inspection procedures should be implemented, to ensure that the completeness, quality and accuracy of the services provided are assured.

The organization needs to include in its agreement with the TTP its rights to all relevant information held and procedures used in the event of the TTP ceasing to trade, or the contract coming to an end. This is to enable the organization to continue to demonstrate compliance over the lifetime of the information, even where a change of TTP has occurred.

Where the TTP is able to demonstrate compliance with the Code, the organization should hold a copy or have suitably controlled access, when required, to the TTP's compliance documentation. The TTP should also be able to demonstrate to the organization that it does, in fact, operate in compliance with the Code.

Whilst it is normal for an organization to deal with a single TTP for a specific document type, it should be recognized that the TTP may need to rely upon a hierarchy or network of TTPs to verify a certificate (see 1.2). Whilst the organization needs to be aware of this, its contractual agreement with the TTP should insulate it from any negative impact (e.g. compromise of a key), where possible, and identify where there has been such an impact.

COMMENT

If a TTP compromises a Private Key, then another TTP may have a claim against the first TTP. In this case, the second TTP's client needs to be protected from this, in line with the third party's agreed contractual liability. This implication of the use of a hierarchy or network of TTPs needs to be clearly understood and accepted by the organization.

KEY ISSUE

> Where TTPs are used, contracts should be signed, and should include appropriate Code compliance statements (see 6.7.2).

3 Planning

3.1 Actions to address risks and opportunities

3.1.1 General

This section of the Code relates to Clause 6 of BS 10008, 'Planning'.

When planning for the authenticity and integrity of information managed by an identity management system, the organization needs to consider the issues referred to in 1.2 and the requirements referred to in 1.3 and determine the risks and opportunities that need to be addressed to:

a) ensure the identity management system can achieve its intended outcome(s);
b) prevent, or reduce, undesired effects; and
c) achieve continual improvement.

The organization also needs to plan:

a) actions to address these risks and opportunities; and
b) how to:
    1) integrate and implement the actions into its identity management system processes; and
    2) evaluate the effectiveness of these actions.

3.1.2 Risk assessment

Identity management procedures are often developed in an unstructured way, by reacting to user requirements, security incidents and/or to available computer software tools. This approach on its own can easily leave gaps in identity management, which are only filled at some later date, typically after a security breach. A more structured approach is to review the identity management systems operated by the organization and assign risk factors (based on asset value, potential threats, system vulnerability and likelihood of attack), on the basis of which appropriate, cost-effective information transfer procedures can be identified. An essential part of identity management is the implementation of an appropriate security policy, which should be produced and approved, based on the risk assessment, and against which security measures can be developed and implemented.

NOTE: A review of this type generally requires security expertise and a range of appropriate technical skills.

The organization should undertake an information security risk assessment along these lines, and document the results obtained. Of particular importance are the security measures implemented to the management of identity. The risk analysis needs to include vulnerability risk factors consistent with the type of identity system used.

On the basis of the results of the risk assessment, existing security measures should be reviewed for effectiveness. Factors such as the balance between the cost of implementation and the security achieved need to be taken into consideration during the review process. Where the review indicates that changes to security measures are appropriate, an action plan should be drawn up with new or amended security measures prioritized for implementation.

KEY ISSUE

> Perform a risk assessment of existing security measures, and implement cost-effective technology and/or procedures to fill any gaps found.

The risk assessment will lead to the acquisition of information and the creation of risk reports. These reports, backed up by the information used to develop the conclusions and recommendations in the reports, may provide useful evidence in relation to the management of identity decisions made by the business.

It is thus important to retain information related to risk assessments in line with an information retention schedule.

KEY ISSUE

> Retain records of risk assessment methods and results in line with the retention schedule.

3.1.3 Risk treatment

The results of the risk assessment should be used to guide and determine the appropriate management action and priorities for managing information risk and implementing controls selected to protect against those risks.

BS ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management* provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

BS ISO/IEC 27005 describes the input to a risk treatment process as a list of identified risks, prioritised according to the organization's risk evaluation criteria. Risk treatment includes the identification and implementation of controls to reduce, retain, avoid or share the identified risks.

Risk treatment can be implemented by one or more of the following non-exclusive processes:

- risk modification;
- risk retention;
- risk avoidance;
- risk sharing.

Risk modification involves the addition, removal or modification of existing controls such that the residual risks can be re-evaluated.

Risk retention is the process of retaining an identified risk without further action. This is acceptable where the identified risk is within the agreed risk criteria.

Risk avoidance involves the removal of processes related to the risk, such that the risk is no longer present. This may be used where the cost of other forms of risk treatment are too costly to implement.

Risk sharing involves the sharing of the identified risks with other parties, such as by insurance or by subcontracting particular processes.

3.2 Objectives and achievements

The organization needs to establish identity management objectives at relevant functions and levels.

The identity management objectives need to:

a) be consistent with the identity management policy;
b) be measurable (if practicable);
c) take into account applicable identity management requirements, and results from risk assessment and risk treatment;
d) be communicated; and
e) be updated as appropriate.

The organization shall retain information on the identity management objectives.

When planning how to achieve its identity management objectives, the organization needs to determine:

a) what will be done;
b) what resources will be required;
c) who will be responsible;
d) when it will be completed; and
e) how the results will be evaluated.

4 Support

4.1 Resources

This section of the Code relates to Clause 7 of BS 10008, 'Support'.

The organization needs to determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the identity management system.

4.2 Competence

The organization needs to:

a) determine the necessary competence of the person(s) doing work under its control that affects its identity management performance;
b) ensure that these persons are competent on the basis of appropriate education, training or experience;
c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
d) retain appropriate documented information as evidence of competence.

NOTE: Applicable actions may include, for example: the provision of training to, the mentoring of or the reassignment of current workers; or the hiring or contracting of competent persons.

4.3 Awareness

Workers doing work under the organization's control shall be aware of:

a) the identity management policy;
b) their contribution to the effectiveness of the identity management system, including the benefits of improved identity management performance; and
c) the implications of not conforming with the identity management system requirements.

4.4 Reporting and communications

It is important when developing policies and procedures to ensure that:

- information related to the policies and procedures is made available to those who are, or may be, affected by them;
- there is a mechanism for feedback from the implementers of the policies and procedures;
- there is a mechanism for reviewing risks related to the policies and procedures;
- details of any challenges to the authenticity and/or integrity of information is fed back to those responsible for compliance with the Code; and
- key individuals responsible for managing communications are identified.

KEY ISSUE

> Ensure that a reporting and communications mechanism is in place, to ensure that new or updated policies and procedures are implemented by all appropriate staff.

4.5 Documentation and records

4.5.1 General

Documented information (also known as records) related to the process of managing information stored electronically needs to be created and retained for as long as is necessary. Section 4.5.2 details procedural documentation that needs to be created and retained. This section also includes information related to the management of this information, including the requirement for version control and appropriate retention periods.

4.5.2 Procedural documentation

4.5.2.1 General

Compliance with the Code requires the availability and use of specified documentation. This documentation consists of the following:

- electronic identity policy statement (see 2.2.2);
- information security policy document (see 2.2.3);
- procedures manual (see 4.5.2.3);
- system description manual (see 4.5.2.4).

The availability of these documents, and demonstrable adherence to the procedures described therein, should, if effectively constructed, provide the audit trail that may be used to demonstrate the authenticity of the electronic identity management systems, and thus enhance the evidential weight of information contained therein.

Note that each of the documents mentioned in the list may actually be maintained as multiple documents, or these documents may be combined. The key recommendation is that the documentation exists, is maintained and is readily accessible to those authorized within the organization to access it and to any authorized third party who may require access. It may also be appropriate to combine this documentation with that developed for compliance with the other parts of BIP 0008.

All documentation needs to be maintained in line with existing working practices, and thus should be maintained under a version control system (see 5.11).

Additional documentation may be required to support the daily operation of the system, for example:

- a system maintenance log (see 5.14);
- an audit trail (see 4.5.3);
- compliance statements (see 6.7.2).

The content of this documentation can easily become unreliable where there are no procedures in place to ensure that it keeps pace with both organizational and system changes. Unreliable documentation may adversely affect legal arguments relating to the correct operation of an electronic identity management system. It is, therefore, important to ensure that the definitive versions of system documents are brought under configuration management control, and are firmly linked to the organization's change management procedures.

Where compliance with the Code is claimed over a period of time during which different editions of the previously listed documentation were appropriate, then all editions of this documentation should be kept, in conformance to the policy document. This is to ensure that, where information regarding the system at a point in the past is required, it can be obtained from this document store.

4.5.2.2 Updating and reviews

It is important to ensure that the procedures implemented at any time during the storage life of any specific electronic document with an associated electronic identity can be determined. This is achieved by ensuring that the procedures manual is kept up to date, and that all previous versions are kept in compliance with the policy statement (see 2.2.2).

KEY ISSUES

> All changes to operational procedures should be managed by a change control procedure, including updating of the procedures manual.
> Superseded versions of the procedures manual should be kept in compliance with BIP 0008-1.
> The procedures manual should be regularly reviewed, to ensure that it is up to date.
> All changes should be reviewed to ensure that compliance with the Code is not compromised.

4.5.2.3 Identity management procedures

The organization should maintain a procedures manual, which should document (or reference) procedures used for operating the electronic identity management systems, to ensure their conformity to the controls detailed in the Code.

The policy document should, for each document type, describe the tools to be used for the association of each of the following attributes, as applicable:

- electronic identity;
- electronic signature;
- electronic copyright;
- confidentiality.

These procedures should specify at what point in the information life cycle these attributes are to be applied and how.

A single document or data file may have more than one such attribute applied, and not necessarily contemporaneously.

A single document or data file may have different attributes applied by different entities.

Where an organization operates a quality management system, such as BS EN ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*, the procedures manual should be included within the quality system.

KEY ISSUE

> A procedures manual should be made available, containing details of (or reference to) other relevant documentation concerning all procedures relevant to the electronic identity management systems.

The procedures manual should include the following topics:

Topic	Action	Section
Keys and certificates	Issuance, acceptance, management, revocation, checking, storage and retention, compromise and key recovery issues	5.3

Topic	Action	Section
Copyright issues	Information ownership, protection and managing change of ownership of copyright documents	5.4
Issuing authority	Management of the authority to issue an attributed electronic information	5.5
Applying information attributes	Issuing procedures for attributed electronic information	5.6
Encryption	Encrypting electronic information	5.9
Compound documents	Handling electronic information that consist of more than one part	5.10
Migration	Management of attributes over time	5.12
System maintenance	Ensuring that the system is reliable	5.14
TTPs	Dealing with TTPs, including procedures, communications, verifications, constraints, Trusted Time, responses, appeals and storage issues	5.15
Version control	Management of multiple versions of documents or data files	5.11

Table 3 – Topics to be included in the procedures manual

4.5.2.4 Key technology components

A description of hardware, software and network elements that comprise an electronic identity management system is required. This should include details of system configuration. The documentation should be structured so that details of the system at any time during the period of its use may be readily accessed. This may be achieved by creating a new version of the manual every time there is a change, or by including a 'change control' section in the manual. What is important is that there is a clear description of the system as it was at a particular time in the past.

For systems already in operation, an electronic identity established prior to the introduction of the Code cannot be considered as meeting its provisions unless the controls and procedures described in the Code have been in place from the time of establishing the identity.

Where the electronic identity policy statement (see 2.2.2) requires compliance with particular national and/or international standards, the system description manual should include a section demonstrating compliance with those standards. This enables system auditors to check the performance and reliability of the system against these standards.

KEY ISSUES

> A system description manual should be made available, containing details of (or reference to other relevant documentation containing details of) all technology-related issues relevant to an electronic identity management system at any point in time.
> Document any standards compliance methodology.

The system description manual should include the following topics.

Topic	Technology	Section
Applying and checking identity	Technology for identity management	5.2.3
Applying copyright protection	Technology for copyright protection	5.4.3
Checking copyright	Determining the copyright status of electronic information	5.4.4
Applying and checking authorization	Management of the authority to add information attributes	5.7
Biometrics	Use of biometric parameters	5.8
Encryption	Description of encryption technology	5.9
Verification requests	The creation of verification requests	5.15.4
Time considerations	Systems for the management of time	5.16

Table 4 – Topics to be included in the system description manual

4.5.3 Audit trails

4.5.3.1 General

When preparing information for use as evidence, it is often necessary to provide further supporting information. This information may include details such as embedded or associated electronic identity and/or copyright protection systems. These details are known as 'information attribute' information.

Audit trail information relating to the management of this attribute information is needed to enable the working of the system to be demonstrated, as well as the progress of information through the organization's systems. Audit trails need to be comprehensive and properly looked after, since without them the integrity and authenticity, and thus the evidential weight, of the attributed information could be called into question.

4.5.3.2 Purpose

The audit trail, as defined for the purposes of the Code, consists of the aggregate of the information necessary to provide a historical record of all significant events associated with electronic identity and/or copyright protection. As such, it covers the answers to all the classic questions concerning the provenance of any electronic information that has been subject to electronic identity management systems.

- Who?
- What?
- Where?
- When?
- Why?
- How?

These audit trail details can be split into two categories:

- system (including the hardware platform(s), applications and operating software, configuration, and processes and procedures); and
- information to which the attributes have been added.

In most organizations, the audit trail will consist of a collection of system- and operator-generated logs.

It is essential that system clocks be synchronized with an accurate time source to ensure that times recorded in audit trails are consistent and reliable.

4.5.3.3 Generation

Audit trail data should, as far as practicable, be generated automatically by the system, and the system description manual (see 4.5.2.4) should describe the processes. In this case, the data should be created and stored immediately after the event that is being audited.

Where audit trail data are not generated automatically by the system, procedures for its manual (or other) generation should be implemented. In this case, the data should be created as soon as possible after the event that is being audited. For example, if the record is of when an operator of an electronic identity management system added an identity to an electronic document, the time should be recorded before the identity is added. If the record is of when preparation of a particular batch of electronic documents was started, the time should be recorded just before the preparation of that batch commences.

It should not be possible to amend any audit trail data. Deletion should be possible only in accordance with the organization's retention policy.

KEY ISSUES

> Audit trail data should be generated automatically wherever possible.
> It should not be possible to alter audit trails.

4.5.3.4 Audit trail content

4.5.3.4.1 General

The audit trail content is critical, as it can be used to audit such activities as the addition of electronic identity and/or copyright protection to an electronic document. Thus, the audit trail needs to include a record of all relevant activities related to the electronic identity management systems. If any significant activity is not audited, then the whole audit trail can be discredited and, as a direct result, it is possible that all or any of the attributed electronic identities will also be discredited.

Thus, technologies for providing electronic identity management systems should be chosen with audit trail requirements in mind. This may result in technologies being rejected that may otherwise have appeared suitable for a particular application.

KEY ISSUE

> When choosing electronic identity management systems, consider suitable audit trail functionality as a basic system requirement.

4.5.3.4.2 Electronic identity management

Records should be kept of historical activities or events that may need to be reconstructed in the future, as additional evidence to support attributed electronic information.

Audit trails should contain sufficient and necessary information to provide evidence of the authenticity of attributed electronic information.

KEY ISSUE

> Audit trails should contain sufficient information to be able to demonstrate all necessary historical activities relating to the electronic identity management systems and to the documents or data files to which the various attributes have been added.

4.5.3.4.3 Attributed information

The audit trail should contain the following information where relevant:

- the time when electronic identity was added;
- the identity of the originator; and
- the system used by the originator.

In some applications, a requirement for confirmed, trusted time stamps is key. Such information should be recorded in the audit trail.

4.5.3.4.4 Identity details

The audit trail should contain the following information where relevant:

- the electronic identity initiator (person, application or device);
- the initiation hardware/software;
- the intended receiver (person, application or device).

4.5.3.4.5 Storage requirements

Where there is a requirement for intermediate or long-term audit information storage, which should be in accordance with BIP 0008-1, sufficient audit information should be stored to enable such time and identity details as are required to be made available.

KEY ISSUE

> Store sufficient related audit trail information to ensure that time and identity details can be determined.

4.5.3.4.6 Date and time

Each audit trail data record should have an associated date and time, which relates to the date and time of the electronic identity management event. This information should be sufficiently accurate that a subsequent investigation can determine the chain of events.

The date and time will normally be that of the creation of the audit trail data, but if this creation is made essentially contemporaneously with the event that is being audited, the time will be to all intents and purposes that of the event itself.

Where a date and time stamp is applied automatically by the system, all changes to the system clock should be recorded in the audit trail. Such changes need to be suitably authorized, and it may be necessary to adjust for daylight saving time or inaccuracy of the clocks.

Where the actual time that an event occurred is important, the use of Trusted Time should be considered (see 5.16).

KEY ISSUE

> Ensure sufficient accuracy of date and time for the application in question.

4.5.3.5 Security of audit trails

4.5.3.5.1 General

The audit trail needs to be secure. If an audit record can be maliciously or inadvertently altered or counterfeited, then the whole audit trail may be discredited and, as a direct result, it may also be possible to discredit all or any attributed electronic information held within the electronic information management system.

4.5.3.5.2 Access

Audit trail information will need to be accessed by authorized operators at relevant times. In some applications, access may only be needed on an ad hoc basis, and thus it is important that the access and interpretation procedures are documented.

There should be procedures for the secure management of audit trail access and interpretation.

Audit trail data should be available for inspection by authorized external personnel (such as auditors) who have little or no familiarity with the system.

Access to the audit trail should, itself, be audited.

KEY ISSUES

> Keep audit trails secure, with audited access only.

4.5.3.5.3 Integrity and protection

If the authenticity of attributed electronic information is questioned, the integrity of the audit trail may be fundamental in establishing the authenticity, and thus the evidential weight, of this information. If the possibility exists that the audit trail data could be modified, this will reduce the evidential weight of any information to which these records apply.

The audit trail should be kept at the level of security appropriate to preventing any change to any data within it, and in accordance with the organization's information security policy (as well as the retention policy and BIP 0008-1).

The audit trail should be subject to internal records management policies and procedures that are at least as good as other 'vital records' of the organization.

Secure backup copies of the audit trail should be kept, including automated and manual audit trail data.

Where file recovery procedures have been implemented as part of the electronic identity management systems, sufficient audit trail data should be stored to demonstrate that the recovery did not affect information authenticity.

For least risk, store audit trail data on 'write-once-read-many' (WORM) media. If a rewritable medium is used, then additional procedures need to be implemented to prevent changes being made. The use of magnetic tape may make it relatively difficult to modify data, as magnetic tape is normally a serially written medium.

If audit trail data have been modified, then any such modification should be audited.

Paper documents used for audit trail data should be removed frequently from the place of use and stored securely. The longer a physical document used for audit trail data (e.g. operator logs) is left in a relatively insecure place, (e.g. at a workstation) the higher the risk of tampering. Users need to assess such risk when using paper for audit trail records. Where paper documents are used, electronic copies of them should be stored on an electronic information management system and in accordance with BIP 0008-1.

KEY ISSUES

> Wherever possible, store audit trail data in an unmodifiable form.
> Where this is not possible, use security measures to ensure that it is not modified.

4.5.3.6 Management

The audit trail needs to be properly managed, as it may be of critical importance to the organization. All claims of compliance with organizational policies may be discredited if the audit trail is not treated correctly and cannot be interpreted unambiguously.

KEY ISSUE

> Ensure that the audit trail data are authentic, accessible, sufficiently comprehensive and understandable.

4.5.3.7 Storage and retention

The storage of audit trail data is a topic often not included in an organization's electronic identity management policies. As they are frequently created automatically, and infrequently accessed, they are usually forgotten and thus not subject to adequate control.

To ensure that all relevant audit trail data are stored, 'audit trail data' should be included as a specific information type in the policy document. They should be stored for at least as long as the information to which they refer is stored, in accordance with BIP 0008-1.

Some systems control the size of audit trail data files by the use of 'looping', which sets the maximum size for the data file, and when this size is reached, new data overwrite the oldest data in the file. Thus, old audit trail data are lost. This process may not be in conformance to required retention periods.

There should be procedures that identify circumstances when an audit trail data file becomes full, and the action to be taken to retain data as required by the retention policy.

Where an organization is working within a BS EN ISO 9000 environment, typically audit trail data relating to compliance with the quality management system are destroyed after a short period of time.

This is not the case with audit trail data from electronic identity management systems, which should be stored for the same period as that of the data to which they relate.

KEY ISSUE

> Ensure that audit trail data are retained for at least the same period as that of the data to which they relate.

4.5.3.8 Format

Frequently, when an organization wants to automate its computer operations environment, it makes use of operating system logs to monitor the electronic identity management systems for specific events or error conditions.

At an application level, ensuring that the application provider uses standard error messages, typically agreed with the organization during the design stage, also enables application status conditions to be monitored.

For example, if an application reads invalid data from a file, rather than just aborting the program with nobody aware of what has happened (until the users raise a support call), if the program writes a status message to an error/system log, in an agreed format, the monitoring software will detect this and notify the user and/or support staff.

These notifications are an important trigger to investigate the continued, proper operation of the electronic document management systems. The entries into the error/system log that caused the monitoring software to raise the alert should be part of the audit trail and should be controlled in accordance with BIP 0008-1.

KEY ISSUE

> Use audit trail formats that enable easy interpretation, both by system users and by automated monitoring tools.

4.5.3.9 Access and interpretation

Access to audit trail information needs to be controlled. In some applications, access may only be needed infrequently, and thus it is important that the interpretation procedures are documented. As audit trail data may be inspected by authorized external personnel (such as auditors) who have little or no familiarity with the system, interpretation procedures should be understandable by non-technical users.

Access to the audit trail should itself be recorded in the audit trail.

KEY ISSUE

> There should be documented procedures that are followed when audit trail data need to be accessed and interpreted.

5 Operation

5.1 Management overview

This section of the Code relates to Clause 8 of BS 10008, 'Operation'.

This chapter deals with the procedures and processes (automated where appropriate) that need to be implemented as part of an electronic identity management system. This will enable the demonstration to internal or external parties that procedures and processes that conform to the Code were in operation at the appropriate times. The actual procedures implemented are to be documented in a procedures manual.

5.2 Technology considerations

5.2.1 General

It is important to utilize reliable and trustworthy technology to facilitate electronic identity management. Technology needs to be chosen with care, offering the appropriate levels of confidence in electronic identity management systems, when compared with the implementation and operational cost of these systems. Technology also needs to be chosen taking into account the possible need to demonstrate 'proper' and 'appropriate' working of the system at some time in the future. This demonstration may need to encompass both the technology itself and the methods by which it was configured and used. Thus, implementers of electronic identity management systems need to ensure that the systems have been designed in accordance with the recommendations of the Code. This chapter contains details of processes that need to be implemented, enabling the defined procedures to be applied.

5.2.2 Electronic identity management technology

Electronic signatures, certificates, authorization, biometrics, encryption, copyright protection and watermarking – these are examples of technologies used to protect information and to enable an electronic identity to be established. This list is constantly changing, however, as new and improved technologies become available. The rate of change of IT will ensure that the techniques used today will be superseded before long.

Thus, one of the key issues to consider and plan for is that enabling technologies will change. In order to be able to answer any challenge in court, documentation therefore needs to be available that describes all the generations of technology that have been used.

Planning for change and migration of information is also a requirement.

INFORMATION – Digital signatures

A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and the integrity of the electronic document to which it is attached or associated can be verified. The algorithm provides the capability to generate and verify signatures. Signature generation makes use of a Private Key to generate a digital signature. Signature verification makes use of a Public Key that corresponds to, but is not the same as, the Private Key. Each user possesses a Private and Public Key pair. Public Keys are assumed to be known to the public in general. Private Keys are never shared. Anyone can verify the signature of a user by employing that user's Public Key. Signature generation can be performed only by the possessor of the user's Private Key.

A hash function is used in the signature generation process to obtain a condensed version of the data to be sent, called a message digest. The message digest is then used to generate the digital signature that is sent to the intended verifier along with the signed data (the message). The verifier of the message and signature re-calculates the message digest and then by using the sender's Public Key verifies both sender and message by comparison with the digital signature (which was created with the matching Private Key). The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data.

The cryptographic hash and signature algorithms are used in combination with cryptographic keys (and padding algorithms) to produce digital signatures.

Signature algorithms include:

- digital signature algorithm (DSA);
- Rivest, Shamir and Adleman algorithm (RSA) as specified in the US Standard ANSI X9.31:1998;
- elliptic curve DSA (ECDSA) as specified in the US Standard ANSI X9.62:2005.

Cryptographic hash functions are detailed in BS ISO/IEC 10118-3:2004, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*.

Typical of such hash functions are:

- MD5;
- RipeMD16;
- Secure Hash Algorithm (SHA), which has a number of variants:
  - SHA-1;
  - SHA-256;
  - SHA-384;
  - SHA-512

  (as defined in the US Federal Information Processing Standards Publication (FIPS PUB) 180-2).

The European Telecommunications Standards Institute (ETSI) has published a special report entitled *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures* (ETSI TS 102 176-1 v2.0.0 (2007-11) http://www.etsi.org/technologies-clusters/technologies/security/electronic-signature).

In addition, the World Wide Web Consortium (W3C) and the IETF have jointly created a standard that describes processing rules and syntax for the use of digital signatures in Extensible Markup Language (XML) documents, http://www.w3.org/TR/xmldsig-properties/ and http://www.w3.org/TR/xmldsig-core2/ (http://www.w3.org/TR/xmldsig-core1/ is still valid for those not yet wishing to move to the latest version (although V2 does have backward compatibility capability)).

A fundamental feature of the XML signature is the ability to sign only specific portions of the XML tree rather than the complete document. This flexibility will be critical in situations where it is important to ensure the integrity of certain portions of an XML document, while leaving open the possibility for other portions of the document to change. Consider, for example, a signed XML form received by a user for completion. If the signature were over the full XML form, any change by the user to the default form values would invalidate the original signature.

The National Institute of Standards and Technology (NIST) is an agency of the US Department of Commerce has published two useful standards:

Digital Signature Standard (DSS) FIPS 186, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf; *Secure Hash Standard* (SHS) FIPS PUB180-4, http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

5.2.3 Applying and checking identity

Electronic identity verification systems may be operated in manual or automatic mode. Where these systems use technologies as part of the verification process, the implemented technology should be documented.

Where it is required to check the identity of the user involved in the verification procedures, or the issue of an associated certificate, the tools to assist in this should be documented.

KEY ISSUE

> Technology used for identity verification should be documented.

5.3 Keys and certificates

5.3.1 Issuance

Procedures implemented when keys and/or certificates are issued for identity and signature use should be documented.

Where electronic signature technology is used, care should be taken in authenticating the original identity, to ensure that it is from the individual or entity being represented.

In all cases, it should be possible to demonstrate which of the processes covered in the Code have been applied to a specific electronic document, whether sourced or received, and know how, when and where to verify this.

COMMENT

Identity fraud is possible because of weaknesses in the registration or enrolment processes, as adopted for issuing documents or certificates used as evidence of identity. The processes used to check identity at the time of use is also an important issue.

According to the UK government document *Registration and Authentication – e-Government Strategy Framework Policy and Guidelines,* Version 3.0, the definition of registration is as follows:

'…the process by which a user gains a credential such as a username or digital certificate for subsequent authentication. This may require the user to present proof of real-world identity (such as birth certificate, passport) and/or proof of other attributes depending on the intended use of the credential (eg proof that an individual works for a particular organisation). Registration can be associated with a real-world identity or can be anonymous or pseudonymous.'

There are two distinct parts to the registration process:

1. validate – demonstrate that a claimed identity exists, that is, that a person, who has certain attributes, exists; and
2. verify – demonstrate that the registrant is whom he or she claims to be, that is, that the person purporting to hold these attributes is not impersonating the actual owner of the identity.

Normally, an identity thief will use a valid identity other than his or her own and will be 'seeking false verification'.

Once obtained, the 'reference' certificates should be accepted and securely stored, in accordance with BIP 0008-1.

Checking of electronic signatures or other underwritten attributes should be performed under the controls of the Code.

When an electronic document or data file originator, authorizer or authenticator is using a digital technique to attach or embed identity and/or signature attributes, for example keys and/or certificates, procedures need to be implemented whereby their issue is controlled, such that the issuing party has a record of what techniques have been used and by whom.

Where it is a requirement that copies of issued keys and certificates are retained securely, procedures that cover the secure transfer and storage of the keys and certificates in accordance with the policy document should be documented.

The key or certificate issuer may require proof of identity as part of the process of issue. If so, such proof should meet the requirements of the relevant information security policy.

EXAMPLE

Registration is the process by which a user gains a credential, such as a username or digital certificate, for subsequent access to electronic services. In many situations it is more important to check the true identity of the organization that employs the individual, than to check the true identity of the individual.

For example, if an electronic identity is required to confirm that an electronic contract has been agreed, the organization's verifiable identity may be more significant than that of the worker. This is the direct analogy to 'for and on behalf of' on so many paper-based contracts. This does not mean there is no significance in the identity of the individual, just that the organization may not be that concerned about whether 'John Smith' really was the worker's name, but will be more concerned that he is the person who works in a particular department with the appropriate responsibilities.

It is also important to understand that the embodiment of identity is not necessarily a person; it may be a particular system, application, process or device within the organization.

The UK government document on organizational identity proof, *Good Practice Guide: Organisation Identity* (GPG 46) requires that the individual acting 'for and on behalf of' the organization should have had their individual identity verified in accordance with *Identity Proofing and Verification of an Individual* (GPG 45).

All records of key and certificate issuance are documents in their own right, and thus should be identified as such and retained in accordance with BIP 0008-1.

COMMENT

The UK government, as part of its publication set surrounding e-government initiatives, has published a document entitled *Identity Assurance: Delivering Trusted Transactions* (https://www.gov.uk/government/publications/identity-assurance-enabling-trusted-transactions) issued by the Cabinet Office to enable the transformation of government and public services to make them more efficient and effective for users. *Good Practice Guide: Requirements for Secure Delivery of Online Public Services* (GPG 43) is particularly relevant (https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services). These specifically address the security requirements related to the provision of registration and authentication services to support access to e-government services. As such, it is essential for all public sector organizations to be fully cognizant of its content and implications. It is also a useful guide for private sector organizations, whether or not they are directly interfacing by electronic means to e-government services, either central or local.

It is important to understand the difference between registration and authentication before looking at how the document ranks the levels required for access to a specific electronic service.

- Registration is the process by which a user gains a credential, such as a username or digital certificate, for subsequent authentication.
- Authentication is the process by which the electronic identity of a user is asserted to, and validated by, an information system for a specific occasion using a credential issued after a registration process.

KEY ISSUES

> Procedures for the issuance of keys and certificates should be documented.
> Key and certificate issuance should be controlled in accordance with the organization's information security policy.
> The relevance of key and/or certificate issuance at an individual or a departmental level should be reviewed.
> Copies of keys and certificates should be securely stored.

5.3.2 Acceptance

Where a document or data file is to be utilized complete with electronic signature and/or copyright, the originator should ensure that the recipient is capable of accurately interpreting the required control.

Procedures to be followed by the user upon receipt of keys and certificates should be documented.

In some circumstances, keys and certificates may not be regarded as valid until a formal acceptance procedure has been completed. In this case, acceptance procedures, and procedures to ensure that keys and certificates are not used prior to the completion of such processes, should be documented.

KEY ISSUE

> There should be procedures relating to the acceptance of keys and certificates by a worker and/or by an organization.

5.3.3 Key management

Procedures for the secure management of encryption and signature keys and/or codes should be documented. This should include key issuance, key retention, key recovery, key updating, key verification, key revocation and key certification procedures.

INFORMATION – Public Key Infrastructure systems

As more and more organizations use digital certificates for user authentication and other security applications, so the number of applications needing to support the use of digital certificates grows exponentially.

Unfortunately, deploying and managing digital certificates across a network is complex, and requires dedicated systems, software, processes and procedures. Without effective management and control, cryptographic keys may be compromised, undermining the security of the system.

Public Key Infrastructure (PKI) systems are available to manage the provisioning and revocation of digital certificates and cryptographic keys.

Care should be exercised before accepting suppliers' claims regarding PKI management, as these systems may be difficult to implement and complex for end user organizations to use. This is because of the sheer scale of provisioning necessary, the number of workers requiring digital certificates and cryptographic keys, key revocation and re-issue, the rate at which workers join and leave the organization and the frequency of changes to their roles and responsibilities.

Keys for encryption may or should not be the same as those for digital signatures. The distinction between keys for encryption and those for authentication of identity and strong electronic signatures using digital signatures should be documented. This segregation of key type and usage can be a useful approach, especially as in some jurisdictions, electronic identity and signatures are allowed but encryption is not, or the cryptographic strength of encryption that is allowed may be different.

An authorized process should exist to identify and react to key compromise (see 5.3.7).

INFORMATION – X.509 standard

The International Telecommunication Union (ITU) ITU-T X.509 recommendation defines what information can go into a (digital) certificate, and describes the data format. See:

http://java.sun.com/j2se/1.5.0/docs/guide/security/cert3.html, and
ITU-T Recommendation X.509 (10/12) Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks,
http://www.itu.int/rec/T-REC-X.509-201210-P/en, which is also issued as an International Standard

(BS ISO/IEC 9594-8:2014, *Information technology — Open Systems Interconnection — The Directory — Public-key and attribute certificate frameworks*).

This Recommendation is summarized on the ITU website as follows:

'Recommendation ITU-T X.509 (BS ISO/IEC 9594-8) defines a framework for public-key certificates and attribute certificates. These frameworks may be used by other standards bodies to profile their application to Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI). Also, this Recommendation (International Standard) defines a framework for the provision of authentication services by Directory to its users. It describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services.'

A usage profile is also available as IETF RFC 5280 (http://www.ietf.org/rfc/rfc5280.txt) (updated by RFC 6818 (http://www.ietf.org/rfc/rfc6818.txt)).

The structure of an X.509 v3 digital certificate is:

Certificate

- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
  - Not Before
  - Not After
- Subject
- Subject Public Key Info
  - Public Key Algorithm
  - Subject Public Key
  - Issuer Unique Identifier (optional)
  - Subject Unique Identifier (optional)
  - Extensions (optional)
- Certificate Signature Algorithm
- Certificate Signature

KEY ISSUE

> Procedures for the management of keys and certificates should be documented.

5.3.4 Revocation

Digital certificates can often be revoked because of compromise, or may simply become out of date. Procedures to be adopted when revoking keys and certificates should be documented.

Keys and certificates may be issued with a pre-set expiry period. Where this is the case, procedures to be followed at the expiry date should be documented in the procedures manual. These procedures should include methods for determining the life span of a particular key or type of key, which may be shorter than that specified by the issuer of the key or certificate.

The procedures to ensure that expired keys or certificates are replaced should be documented. There may be a requirement to retain 'time expired' keys and certificates, to ensure that future challenges to identity may be sustained. Procedures to meet these requirements should be documented.

Time is one factor whereby an issued key or certificate may no longer be relied upon or used. In some other circumstances, alternative revocation mechanisms will be necessary to meet the policy requirements (examples of this include staff leaving employment, removal of authority or security compromise). To cover these circumstances, procedures and authority whereby keys or certificates are revoked should be documented.

These procedures should also indicate whether documents signed with keys and certificates after they have been revoked are identified and whether necessary actions have been taken.

For most revocations, it is important that an agreed time of effect is included. This should be unambiguous and may, in some circumstances, need to rely upon an underwritten Trusted Time stamp.

KEY ISSUE

> Procedures for the revocation of keys and certificates, whether due to time or security issues, should be documented

5.3.5 Checking

Procedures for the confirmation of the authenticity of a key and/or certificate should be documented. These procedures may, in some cases, require that keys and certificates are confirmed at a specific point in a document life cycle.

Procedures for the recording of responses received from a check and the action to be taken on receipt of a response should be documented. For example, if a check indicates that a certificate was not valid at the point in time in question, the action to be taken needs to be clearly understood.

In some circumstances, guarantees given by the key or certificate issuer will be sufficient to enable checking to be an exception, rather than a normal event. Some technological approaches are better suited to this than others.

Whilst for some specific document types it may be desirable to delay checking until there is a dispute rather than at the earliest possible opportunity, this may not necessarily be an acceptable process. This could be because the time lag before checking makes the cost or complexity of the delayed check excessive or infeasible.

KEY ISSUES

> Procedures for the checking of keys and certificates should be documented.
> Procedures for responding to a failed check should be documented.

5.3.6 Storage and retention

Procedures for the secure storage and retention of keys and/or certificates should be documented.

Procedures used to ensure the confidentiality of Private Keys should be documented. Where Public Keys are concerned, there may be little value in storing those keys confidentially. The same is not, however, true for Private Keys.

The key or certificate issuer may limit its liability, in the event of an actual or potential key compromise, or indeed if the key has not been retained with sufficient care and attention. The user should understand the implications of such limits and may well use such criteria to review whether the appropriate controls are in place or whether the key or certificate issuers' limits are indeed acceptable.

In some countries (or other relevant geographical areas) legislation has been enacted or is being considered that specifies that keys and certificates need to be securely retained by a nominated third party (escrow) or be capable of being recreated (key recovery) by appointed agents. Where such requirements exist, appropriate procedures should be documented.

KEY ISSUES

> Procedures for the storage and retention of keys should be documented.
> Where escrow or key recovery procedures are used, the procedures should be documented.

5.3.7 Compromise

Procedures to be followed in the event of actual or suspected compromise of key and/or certificate or certificate or registration authority (CA or RA) should be documented. These procedures should include details of who should be notified and how the notification should be registered.

KEY ISSUES

> Procedures to be followed in the event of key and/or certificate compromise should be documented.
> Procedures to be followed in the event of certificate or registration authority compromise should be documented.

5.3.8 Key recovery

Procedures to be implemented where a key is to be recreated or otherwise recovered should be documented. Such key recovery procedures may be required as a result of the loss of a key, or because access to that key is no longer feasible, for example a departing, disgruntled worker has made the key inaccessible or has corrupted it.

Where a third party has a legitimate requirement to perform key recovery, or has the right of access to the unencrypted version of an encrypted document, the procedures and authorization may be those specified by that third party or may be subject to legislative or regulatory controls.

EXAMPLE

Legislation may exist mandating, under certain circumstances, disclosure of message content.

An example of this in England and Wales is the Regulation of Investigatory Powers Act 2000, which:

'introduces a power to enable properly authorised persons (such as members of the law enforcement, security and intelligence agencies) to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information which they lawfully hold, or are likely to, in an intelligible form.'

Explanatory Notes referring to section 49 of the Act

Furthermore, the Act also covers the disclosure of encryption keys used when messages are sent in encrypted form.

The disclosure of the encrypted message and the keys may be a necessity to establish that the 'intelligible form' was, in fact, the actual encrypted message transmitted.

Where key recovery has been performed, the recovered keys should be treated in the same manner as any other keys.

KEY ISSUE

> Procedures for the recovery or recreation of keys should be documented.

5.4 Copyright issues

5.4.1 Information ownership

The organization should assess where there may be a requirement to demonstrate copyright ownership in relation to particular documents or data files. Such a process can be used to add evidence of the identity of the copyright holder of particular information.

Where the copyright of documents or data files created by a worker during the course of his or her employment is to be assigned to the organization, workers' terms of employment should be used to ensure that the organization owns the copyright.

Where assignment of copyright to the organization may be unclear, procedures should be documented for its verification.

Procedures should be documented that review the impact and risk of inadvertent or malicious copyright infringement, and how the risk can be minimized.

INFORMATION – Copyright

Copyright is internationally recognized. The Berne Convention for the Protection of Literary and Artistic Works covers the international aspects of copyright. It is not, however, recognized in every country and state. This may, or may not, be a concern for particular types of document.

Copyright subsists the moment a work has been created and can last beyond the lifetime of the author (the time may vary between countries and states). Thus, any document, letter, email, contract, article, etc. will be subject to copyright protection. Such protection is not restricted to artistic or literary works.

Copyright ownership is normally with the creator, even when work is performed under a commission. The creator may be an individual or an organization.

Typical digital copyright protection technology will show document origination, even if only part of an original is copied. The technology may also resist digital/analogue transformation and manipulation of protected documents.

KEY ISSUE

> Procedures for assigning copyright ownership of documents should be documented.

5.4.2 Copyright protection

Procedures should be documented which ensure that copyright protection is implemented in accordance with the requirements of the policy document.

These procedures should include:

- copyright statements linked/added to documents and data files;
- dated copyright notices;
- unambiguously specified copyright ownership;
- the secure retention of the original document, or an authenticated copy, in accordance with BIP 0008-1; and
- copyright ownership bound to the copyright document or data file.

The organization should also document, where appropriate, procedures to:

- lodge the original information, or an authenticated copy, with a TTP (if lodged by electronic transfer this should be under the controls of BIP 0008-2);
- register the copyright with a suitable, TTP;
- add digital copyright protection technology to the original information (or authenticated copy); and
- have the copyright notice independently verified or notarized.

The copyright holder should assess the level of risk being accepted in relation to potential copyright compromise, and document relevant procedures.

If, as a result of the organization's risk assessment, copyright protection systems are required to be implemented for a particular information type, then relevant procedures to ensure that copyright protection is applied should be documented.

Procedures should be documented for use when external contact needs to be made for checking copyright.

Procedures should be documented which ensure that the copyright owner informs the information user if any trusted third-party organization or copyright protection system has been used, to simplify copyright checking and report copyright licence use or abuse.

KEY ISSUES

> Appropriate copyright protection systems should be implemented.
> Procedures to be followed in the event of compromise should be documented.

5.4.3 Applying copyright protection

The processes inherent in implemented copyright protection systems should be documented. This documentation should include details of how copyright protection is applied to different types of document.

The following attributes of copyright protection systems should be included in the documentation as applicable:

- copyright ownership;
- copyright date;
- watermarking;
- registration of the copyright (with the copyright protection system supplier or other third party);
- secure archiving of the copyright material (with the copyright protection system supplier or other third party);
- copyright licence terms;

- copyright marking;
- copyright statement addition;
- bonding statements, marks, ownership, dates, etc. to the copyright material (this may be by the use of digital signature techniques).

INFORMATION – Note

Some copyright protection systems include subsystems for reporting licensed usage of copyright material. Such reporting and licence fee recovery is outside the scope of the Code, but may be important areas for consideration.

KEY ISSUE

> The technologies used for copyright protection should be documented.

5.4.4 Checking copyright

Automatic and manual processes for the checking and confirmation of copyright ownership of a document or data file should be documented.

Where it is required to check the copyright ownership, date, integrity, identity of the copyright holder, etc., tools used to assist in this process should be documented.

KEY ISSUE

> Technology used for checking copyright ownership should be documented.

5.4.5 Status change

Copyright on a document or data file has a time limit and, therefore, the creation or publication date of copyright material should be recorded.

At the end of the copyright time limit, copyright is no longer valid or enforceable. It is not the responsibility of the original holder of the copyright to notify status change.

There may be circumstances where certain document or data file types need to have their copyright status changed, for example, where a change in the 'licence to use' terms occurs. Where these circumstances may occur, there should be procedures that specify the authority level necessary to approve such a status change and detail the notification that should accompany a change of copyright status.

KEY ISSUE

> In addition to the normal date-activated loss of copyright where a change of copyright status may occur, such changes should be documented.

5.5 Issuing authority

An organization is responsible for ensuring that documents are properly authorized, otherwise it may not meet legal requirements because of lack of internal controls. The principles that, for example, apply to the control of signing important documents need to be applied to their electronic equivalent.

INFORMATION – Sarbanes—Oxley Act

The Sarbanes—Oxley Act of 2002 (SOX) in the USA was introduced in the wake of the well-publicized problems at Enron and other organizations. Whilst it is focused on US businesses, its scope is wide enough to include many UK and European firms.

The SOX holds CEOs and CFOs personally responsible for corporate wrongdoing. The Act requires organizations to demonstrate that auditing is performed, and that records cannot be altered, concealed or destroyed. The Act directly requires company CEOs and CFOs to sign off on the results of financial reports, which have a heavy reliance on income and revenue statements from corporate information systems covering expenditure as well as sales.

A key section of SOX (section 404) addresses internal controls, and effective record keeping is the foundation for this requirement. There is a strong correlation between these requirements and those stated in the UK *Corporate Governance Code*, published by the Financial Reporting Council (FRC) (www.frc.org.uk/corporate/ukcgcode.cfm).

The FRC have also published a guide using the Turnbull Guidance (now known as *Internal Control: Revised Guidance for Directors on the Combined Code*) to comply with Section 404 of SOX,
www.frc.org.uk/getattachment/5e4d12e4-a94f-4186-9d6f-19e17aeb5351/Turnbull-guidance-October-2005.aspx

The method of, and authority for, granting and issuing such authority levels for document issue should be documented.

INFORMATION – Financial Reporting Council: corporate governance

The FRC is the UK's independent regulator responsible for promoting high quality corporate governance and reporting to foster investment. The FRC sets the framework of codes and standards for the accounting, auditing, actuarial and investor communities and oversees the conduct of the professionals involved.

Key FRC publications include:

The UK Corporate Governance Code (formerly known as *The Combined Code*)
www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-2014.pdf;
The UK Approach to Corporate Governance
www.frc.org.uk/Our-Work/Publications/Corporate-Governance/The-UK-Approach-to-Corporate-Governance.pdf;
Internal Control: Revised Guidance for Directors on the Combined Code (formerly known as the *Turnbull Guidance*)
www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Turnbull-guidance-October-2005.pdf.

The level of authority required for the issuing of specific types of document should be documented.

EXAMPLE

Whilst it is clear that not all staff within an organization have the authority to issue payment approvals, the procedures for granting authority to approve such payments need to be documented.

Where appropriate, these procedures should be made clear to other users of the document, within and outside the organization.

EXAMPLE

A workflow process change may only be allowed by a top manager of the organization. These procedures need to include the approval of this authority level. In the event of a dispute in the future, the query raised might be 'Was this specific individual a top manager at that time?'

KEY ISSUE

> Issuing authority levels for specific document types should be documented.

5.6 Applying information attributes

It is important that the techniques used to apply or inextricably link electronic identity, signatures and/or copyright to electronic information, possibly in a confidential manner, by an organization or an individual, are clearly understood and controlled by the organization or individual in question.

Procedures should be documented that allow an approved individual to apply an electronic identity, signature and/or copyright technique to electronic information. These procedures should include the recording of the identity of the person applying such a technique.

Procedures should be documented which ensure that an electronic identity, signature and/or copyright technique is not inadvertently applied.

Procedures should be documented which ensure that all relevant information attributes are applied. There may well be a balance between the risk of not immediately checking authenticity and the cost of checking everything immediately. This needs to be assessed and accepted/rejected as appropriate.

KEY ISSUE

> There should be procedures for applying keys, certificates and/or copyright techniques to electronic information.

5.7 Applying and checking authorization

Electronic signatures and certificates or other cryptographic checksum techniques may be used to demonstrate that the information authority may be relied upon.

The techniques utilized, the point at which the technique is applied to a specific information and when the authority is checked by reference back to the technique should all be documented.

Where it is required to check the identity of the user involved in the identity verification procedures, or the issue of an associated certificate, the tools used to assist in this should be documented.

In some circumstances, authorization is required to facilitate information status change, for example, when information passes from one workflow process to another. As long as the access controls and management and audit records are suitable, the evidence of transition from one workflow stage to another (which is thus associated with the authority of the transition) may provide demonstrable authorization.

If the authorization is being considered by another organization, it is essential that the originating organization ensures that the other is capable of interpreting the authorization and the commitment it carries.

KEY ISSUE

> Technologies used in authorization applications and/or checking should be documented.

5.8 Biometrics

Biometrics can be used in electronic identity management systems and relate to the physical attributes of an individual such as a fingerprint or a DNA sample. Biometrics can be used to demonstrate that the identity of an individual is the same as when the biometrics of that individual were first established, by reference to the same checkable physical attributes.

EXAMPLE

Authentication security solutions use one or more of three fundamental factors to authenticate identity that are not available to other people:

- something you know – such as passwords, mother's maiden name, or place of birth;
- something you have – key, ID card, USB fob or smart card;
- something you are – biometrics using, retinal scan, fingerprint, gait, voice etc.

These factors are often, however, vulnerable to attack.

For example, policies for ensuring secure passwords result in greater inconvenience for users, in turn causing users to write down the passwords or use passwords that can be easily memorized. In addition, typical users use the same password for multiple accounts, further degrading security. Password cracking tools are readily available for download from the internet, making it relatively easy to crack the typical password. Furthermore, many successful attacks are accomplished using passwords or other personal secrets obtained from social engineering, a problem that even the best of security policies find difficult to address.

Consider the combination of a password and a hardware token. Systems using this form of two-factor authentication are vulnerable to attacks through theft of the hardware token coupled with the use of social engineering to obtain the user's password.

By using a biometric as well, the result is 'three factor' authentication, virtually eliminating the vulnerabilities of 'one factor' and 'two factor' authentication systems. If a biometric is used along with a password but without the hardware token the authentication is only 'two factor' but is not vulnerable to loss of the token.

Different biometric tests perform identity verification functions with various degrees of confidence.

A biometric does not generally prove that the individual is who he or she purports to be. If rigorous checks are performed to check real identity at the time a biometric is issued, however, then much more confidence may be placed in the individual's true identity when the biometric is subsequently used to authenticate an individual. In this case, the associated risk of mis-identification will be reduced.

EXAMPLE

The fingerprint is considered difficult to forge. However, if you believe my name is Smith (when in fact it is Jones) at the time my fingerprint is recorded, there is no inference from my fingerprint that I am Jones, and the biometric will just link me to the 'false' identity, Smith.

An identity link is likely to be dependent on the strength of the biometric, the strength of the identity check and the strength of the security protection of these items and their linkage. The organization should review any liability for an erroneous match of a biometric.

There are many biometrics, for example:

- signatures (not to be confused with the scanned image of a signature);
- fingerprints;
- face images;
- iris/retinal scans;
- hand/palm/foot/ear prints;
- gait;
- voice;
- DNA.

Biometrics may be used to supplement or supplant passwords or PINs.

The organization should assess the requirements for identification of individuals, and should select an appropriate biometric where appropriate.

COMMENT

Which biometric should be chosen, and what are the rates of false positives and false negatives to be expected in operational use? The nature of biometrics is such that the biometric at authentication checking is compared with that captured at (for example) enrolment or registration. A comparison is made that will generally give a 'confidence level', usually in the form of a 'score'. The user organization should then set score levels for rejection or acceptance. These can be set at different levels for different transactions; for instance, the confidence level for 'view only' access to a data set may be less than an 'update' to the same information. The more rigorous the sampling taken at the initial authentication, the lower the rates of false negatives or false positives will be for a given confidence level. More rigorous sampling will typically, however, be more expensive in terms of either time or equipment.

A balance, based on the organization's risk analysis, must be made.

The technology used to establish and check the biometrics of an individual should be documented. This documentation should include any processes used to check actual identity, or not, to appropriate levels of confidence.

KEY ISSUE

> Where biometrics are used in electronic identity checking systems, the technology used should be documented.

5.9 Encryption

5.9.1 General

Encryption can be used for confidentiality purposes, perhaps as part of the copyright protection process, or to improve the security and integrity of an electronic document or data file. Where encryption is used, procedures for its application, control, management of keys, audit, etc. should be documented. These procedures should take into account local and international legal issues that may specify controlled access to unencrypted forms of the encrypted documents or to encryption keys.

Encryption keys, which should be different from digital signature keys, should be kept securely, such that they are available only to authorized persons.

Encryption key allocation and issuance procedures should be documented. These keys may be issued to devices, applications or services as well as to people.

Where third-party key management facilities are used, relevant procedures should be documented. Procedures that ensure the continued availability of keys and certificates should be documented.

These procedures need to include arrangements for the off-site storage of keys and certificates for disaster recovery purposes. This is best managed as part of the business continuity plan.

KEY ISSUE

> Encryption keys should be managed in a secure way, and should be included in the organization's business continuity plan.

5.9.2 Techniques

Where encryption techniques are employed as part of an electronic identity management system, they should be available to the appropriate organizations (originator and receiver), irrespective of (but not in contravention of) the respective national legislation and/or licensing situations.

Encryption techniques and technologies should be documented. This documentation should include necessary reference to the algorithms, key generation, recovery and management, and certification processes.

Key escrow and/or key recovery procedures and access rights to the encryption keys should be included in the documentation.

KEY ISSUE

> Where encryption technologies are used, they should be documented.

5.10 Compound documents

A compound document is a document that is made up of two or more parts, each of which can exist as a separate entity. For such documents, the identity associated with copyright, authentication and authorization may be applied to the whole document or to specific parts thereof.

INFORMATION – XML

XML is a major enabler of what the internet and web services require in order to continue growing and developing as an environment for trustworthy electronic transactions. A lot of work remains to be done on security-related issues before the full capabilities of XML languages are realized. At present, the most important sets of developing specifications in the area of XML-related security are:

- XML encryption (www.w3.org/TR/xmlenc-core1/), XML digital signatures (www.w3.org/TR/xmldsig-core1/, also see ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES);
- XML Access Control Language or Extensible Access Control Markup Language (XACML), an OASIS Standard (http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf);
- SAML (Security Assertions Markup Language), an OASIS Standard, (http://saml.xml.org/saml-specifications);
- XKMS (XML Key Management Specification - Version 2.0) (www.w3.org/TR/2005/REC-xkms2-20050628/).

Encrypting a complete XML document, testing its integrity and confirming the authenticity of its sender is a straightforward process. But it is becoming increasingly necessary to use these functions on specific parts of documents rather than the complete XML document, to encrypt and authenticate in arbitrary sequences, and to involve different users or originators.

This may mean, for example, that parts of an XML document are ‘in clear’ whilst those parts that contain personal data are encrypted.

For each document type, it should be unambiguous as to which parts, or the whole, require and have the identity associated with copyright, authorization or authentication applied.

KEY ISSUE

> Where compound documents are involved, keys, certificates and/or copyright can be assigned to individual components and/or to the whole document.

5.11 Version control

All hardware, software and procedural documentation used in conjunction with the Code should be maintained under a version control system.

Such a system should include the keeping of appropriate records of changes made and should enable relevant information about the configuration of the electronic identity management systems at any time in the past to be reviewed.

KEY ISSUE

> Keep records of all procedural and process documentation in accordance with a retention policy. This is to enable the configuration and use of the system at any point in the past to be demonstrated.

5.12 Migration

When keys and certificates are superseded or when signature, encryption and copyright protection techniques are upgraded, it is essential that the records and algorithms that are necessary to verify copyright, authentication or authorization in disputes are retained. The details will, however, be dependent on the use of the old and new processes and technologies.

A procedure should be developed for the planning process for future migration projects. The plan should detail the requirements of the testing process to be carried out and the manner in which specific migration plans and test results are to be retained.

When any migration is undertaken, the 'transfer' processes should be agreed prior to introduction. The course of the transfer should be audited along with a demonstration that results are meeting expectations. The results of migration should be retained in accordance with BIP 0008-1.

When forms of demonstration of identity are to be changed, then the identity vested in existing electronic information needs to be considered. The impact of changes needs to be assessed, and procedures for confirmation of the identity of electronic documents and data files under the control of superseded systems, in the light of replacement systems, need to be considered and accepted as appropriate.

KEY ISSUE

> Migration projects should be planned and documented, such that it can be demonstrated that keys, certificates and copyright have not been compromised.

5.13 Business continuity planning

The unavailability of keys and certificates for electronic identity and authentication (even for a matter of minutes in some applications) can be a serious problem for organizations. Thus, procedures are required that can be implemented to control and minimize the impact of such a situation.

Business continuity of keys and certificates for electronic identity and authentication is not managed simply by the availability of suitable alternative facilities, as the unavailability of premises, staff and/or hardware needs to be included too. Such procedures may involve the temporary use of additional or third-party resources.

In order to ensure that the integrity and availability of information, keys and certificates are not compromised during a loss of service, an agreed and approved business continuity plan (sometimes known as a disaster recovery plan) should be implemented that covers these areas.

Business continuity procedures should be established in relation to keys and certificates, to:

- cope with major equipment, environmental or personnel failure;
- include the testing of such procedures;
- include the maintenance and upgrading of such procedures; and
- ensure that such procedures do not compromise the integrity of information during their implementation.

Where TTPs are used, their services should be included in the business continuity plans.

The organization should verify that the business continuity plans of trusted third-party service providers meet its requirements.

KEY ISSUES

> Business continuity plans in relation to keys and certificates should be agreed and tested.
> Where TTPs are used, their business continuity plans should meet the requirements of the organization's business continuity arrangements.

5.14 System maintenance

An electronic identity management system should be maintained by qualified and trained personnel to ensure that its performance does not deteriorate.

A maintenance log should be kept, detailing all preventive and corrective maintenance procedures completed.

Procedures for preventive maintenance should be documented. These procedures may be performed by system operators, or by specialized service personnel.

KEY ISSUE

> Where maintenance (corrective or preventive) is required, it should be carried out by trained personnel.

5.15 Trusted third parties (TTPs)

5.15.1 General

This section is to be used where TTPs are used. TTPs provide trust services to the organization, for example, they are able to verify certificates and signatures. These services may be made available using dedicated connectivity, using public switched networks or across the internet (cloud).

See also BIP 0008-2 for further discussion on third parties.

5.15.2 Procedures

Where the TTP is able to demonstrate the implementation of procedures that conform to the Code, any contract with it need only confirm this situation and include agreed procedures for checking compliance.

The following defines procedures and processes that need to be reviewed and included within the contract as appropriate. The organization should check that:

- the service provider can produce verifications to agreed acceptable standards of response times and service availability levels;
- the TTP can process a sample of test verifications, which can be successfully responded to on the organization's target system. This sample should be retained;
- the TTP can provide access to, or supply a copy of, the audit trails of the processing undertaken, in an acceptable form;

- the proposed location of the work is acceptable and meets security criteria appropriate to the organization's needs;
- the proposed procedures and processes involve no greater security risk than its own procedures;
- where security of the material to be processed is important, the service provider can vouch for the trustworthiness of the intended operational staff.

COMMENT

As previously stated in the Introduction, tScheme is the independent, industry-led, self-regulatory scheme set up to create strict assessment criteria, against which it will approve trust services.

To assist with this it has created Approvals Profiles for providers of trust services for PKI related services and non-PKI related services. These can be found at www.tscheme.org/profiles/index.html

There is also a *Guide to Securing Electronic Transactions* (tSi0256) in the tScheme Library www.tscheme.org/library/index.html#guidelines

KEY ISSUE

> Procedures for the management of trusted third-party services should be documented.

The organization shall establish procedures to be utilized in the event of the TTP ceasing to operate (with or without due notice to the organization).

The organization shall establish procedures to be followed in the event of a failure of the trust service provider's security (e.g. a CA is compromised by attack and false certificates are issued by the compromise perpetrators as was the case with DigiNotar).

INFORMATION

NIST have published guidance on preparing for and responding to CA compromise: http://csrc.nist.gov/publications/nistbul/july-2012_itl-bulletin.pdf

5.15.3 Transfers

Where a TTP receives information (such as digital signature keys or encryption keys) in order to provide verification services, secure procedures should be implemented for this transfer in accordance with the recommendations of BIP 0008-2.

COMMENT

One area that TTPs will frequently have covered in their security policy is that electronic communications with them should be over secure, encrypted channels. This will prevent eavesdropping on the message and will allow them to authenticate the identity of the person or system accessing their systems. This will frequently use either secure sockets layer (SSL) or transport layer security (TLS).

Such use of a secure channel is also often used for secure mail applications or access to webmail services. A number of secure email services are based on the approach of sending links to messages held on secure web servers, using normal email services. Recipients follow the links using their browser and will only be able to access the confidential messages over an SSL or TLS protected channel, which will only be opened up to them when they have successfully identified themselves as the intended recipient. It should be noted, however, that such secure channels may mean that information is not checked by the organization's boundary defences intended to prevent access to inappropriate or dangerous material.

Similarly, where the organization receives information (such as responses from a TTP) in order to substantiate verification, secure procedures should be implemented for their receipt in accordance with the recommendations of BIP 0008-2.

These types of transferred information may need to be retained, in which case it should be in accordance with BIP 0008-1.

KEY ISSUE

> Methods for securely communicating with a TTP should be documented.

5.15.4 Verification requests

5.15.4.1 Procedures

The organization needs to have procedures defined and documented that are to be followed when a digital certificate or a copyright protection certificate needs to be verified. These procedures need to include such action as may be required in the event of a challenge to the authenticity of a certificate or other verification.

The procedures should detail, for each information type, the information required and authority necessary to submit to the appropriate TTP a request for verification of a certificate.

Verification requests should be made under secure conditions, as defined by the organization's information security policy (see 2.2.3.4).

The agreement with the TTP should include an agreed procedure for submitting, and responding to, verification requests. The agreement should also include procedures for ensuring that requests are valid and have been initiated by an authorized individual, application, service or device.

Verification requests that do not conform to contractual requirements should not be responded to. Where multiple TTPs are used, separate procedures may be needed for each TTP.

The information required should include:

- the identity of the certificate for which verification is requested;
- the identity of the requestor with details of authority;
- the date and time of the verification request;
- any other details of the request;
- the trusted third-party access codes;
- the required response priority/time-frame.

All documentation produced for, or as a result of, such a request should be treated by the organization as a part of the document being verified and should be retained in accordance with the recommendations of BIP 0008-1, and associated with the document or data file to which it refers.

Where a request for verification is issued electronically, it should be transferred to the TTP in accordance with the recommendations of BIP 0008-2.

KEY ISSUE

> Procedures for the requesting of verification should be documented. Verification requests should be made under secure conditions.

5.15.4.2 Technology

Where technology is used to generate verification requests, it should be documented.

Where authority to create verification requests is controlled by technology, the hardware/software used for this process should be documented.

Where verification requests are transferred electronically, the hardware/software used for this process should be documented.

KEY ISSUE

> Technologies used to create and transmit verification requests should be documented.

5.15.4.3 Timing of verification

Procedures for the determination of the requirement for a verification of a certificate should be documented.

It may be necessary to verify certificates as soon as the information is available at a defined point in its process model, for example at receipt of transfers. Where immediate verification is required, automatic timely reference to the TTP should be considered and, if appropriate, implemented.

For other information, it may be unnecessary to check unless and until there is a dispute. There may be limits to the time that the TTP is able, or willing, to spend in responding to verification requests; this should be a consideration in the process specification. This should be considered if documents are to be retained for a long period under the controls of BIP 0008-1.

Many information types may fall between these two extremes of immediate verification or delay until a dispute arises; in such cases, a delayed verification may be appropriate and verifications could be batched together. The maximum delay time should be defined for each information type where this approach is adopted.

KEY ISSUE

> The step in a business process where verification is required should be documented.

5.15.5 Authorization

The agreement between the organization and the TTP should specify the authorized individuals, services, applications and devices that may issue a verification request. Procedures should be implemented in which the identities of the authorized entities are included within the verification request documentation.

Organizations should ensure that only authorized individuals can request verifications.

KEY ISSUE

> Authorizations for making verification requests should be communicated with the TTP.

5.15.6 Request constraints

The agreement with the TTP may include a number of request constraints. These need to be acceptable to both parties and be included as part of the agreement.

COMMENT

The TTP may only be available for access from specific geographical areas or for specified hours of the day, or may only agree to verify certificates issued in a certain geographical area or time-frame, for example within a specified time of the use of the certificate.

Another constraint may be the level of underwriting that the TTP is prepared to give to different certificate types or to the certificates issued by other TTPs. This latter area, known as 'cross certification' may well attract different terms and conditions from the TTP.

Procedures should be such that any request constraints are identified and actioned as appropriate.

KEY ISSUE

> Procedures that ensure that request constraints are managed should be documented.

5.15.7 Trusted Time

Where there is a particular need to demonstrate the accuracy of date and time stamps associated with verification requests or responses, the use of trusted third-party services for the verification of time should be considered and implemented, if appropriate.

Where Trusted Time is used, procedures for demonstrating the integrity and authenticity of a time stamp and its binding to a particular piece of information should be documented.

DEFINITION

Trusted Time is time that is certified to be traceable to the legal time source for the application in which it is being used and is not forgeable either at the time of initial use or anytime in the future.

RFC 3161 (and RFC 5816 (www.ietf.org/rfc/rfc5816.txt)) are the IETF PKI Time Stamping Protocol specifications (www.ietf.org/rfc/rfc3161.txt) which are extended in ANSI X9.95 2012, *Trusted Time Stamp Management and Security* for the management and security of trusted time stamps, http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.95-2012

RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)* describes the format of a request sent to a Time Stamping Authority (TSA) and of the response that is returned. It also establishes several security-relevant requirements for TSA operation, with regards to processing requests to generate responses.

A time-stamping service supports assertions of proof that a datum existed before a particular time. A TSA may be operated as a TTP service, though other operational models may be appropriate, for example an organization might require a TSA for internal time-stamping purposes.[2]

Another useful source is the technical specification published by ETSI entitled *Electronic Signatures and Infrastructures* (*ESI*); *Policy Requirements for Time-stamping Authorities* (ETSI TS 102 023 V1.2.2 (2008-10) www.etsi.org).

The provision of Trusted Time may be by the TTP, by another third party on behalf of the TTP, or by another different TTP. In some cases, the organization may operate its own time-stamping system.

KEY ISSUE

> Where accurate and verifiable time is required, the use of Trusted Time should be considered.

5.15.8 Response handling

Procedures that detail all the possible responses to a verification request, including their format and content, should be documented.

These details should be listed or referenced in the agreement with the TTP. Procedures detailing the action to be taken by the organization upon receipt of a response to a verification, whatever the content of the response, from the set of possible options, should be documented.

COMMENT

In the event of an unexpected request for verification, or for any form of information, the organization must have a pre-arranged process in place to react according to the specific requirements of the business for the transaction in question. Whilst the TTP should not be responding in any manner outside the agreement with the organization, there may be circumstances where the TTP or the organization has an undocumented system 'feature' or has failed with its change control procedures.

Plan for the unexpected!

Procedures for the action to be taken by the organization in the event of receiving a response from the TTP that does not conform to agreed format or content should be documented.

Procedures for the authentication of responses, to ensure that they have been approved by the TTP, and that their integrity has not been compromised prior to receipt, should be documented.

All responses should be unambiguously linked back to the verification requests to which they refer.

Where the response is issued electronically, it should be transferred by the TTP under the controls of BIP 0008-2.

The response should be stored by the organization in accordance with the policy document, under the controls of BIP 0008-1.

[2] See http://www.ietf.org/rfc/rfc3161.txt?number=3161

KEY ISSUES

> Procedures for the handling of responses to verification requests should be documented.
> These procedures should include the handling of unexpected responses.

5.15.9 Response constraints

The agreement with the TTP may include a number of response constraints. These constraints need to be acceptable to both parties and be included as part of the agreement.

COMMENT

The TTP may have had a report of compromise of a key that may lead to certificate revocation.

Procedures should be such that any response constraints are identified and actioned as appropriate.

If a verification request refers to a key or certificate that is already the subject of a notice of compromise, then a notification to the organization should be sent from the TTP of the doubts over the validity of the request.

If the compromise was reported after the verification request was sent to the TTP, then a notification should be sent by the TTP to the organization with information about the suspected compromise and the potential invalidity of the previous response.

Another example of a response constraint is that the TTP may limit the time between issuance of keys and certificates and verification. This may be because of its desire to avoid holding information for excessively long periods.

Clearly, in this case the organization needs to ensure that its required checks on validity are performed during the period that the TTP has specified.

NOTE: Many TTPs may want to adopt retention periods for information that may be shorter than the requirements of the organization for a specific document type.

KEY ISSUE

> Procedures for dealing with request constraints should be documented.

5.15.10 Appeals

The agreement between the organization and the TTP should include references to procedures to be followed in the event of a dispute, for example, as a result of non-achievement of committed service levels.

The organization also needs defined procedures to be implemented where a TTP is unable to provide satisfactory evidence when requested.

These procedures may also be used in the event of noncompliance by either party, when the TTP challenges the authority of a verification request, or when the organization has grounds to dispute the response to a verification request.

COMMENT

Much of the basis for dispute resolution should be contained in the contract with the TTP or the documents referred to by it, such as the certificate policy and the CPS. It should be recognized, however, that these will, in all probability, limit the liability of the TTP.

Where the TTP has been accredited by an independent body, such as tScheme, then that body may well wish to ensure that disputes are resolved promptly and without damage to the reputation of the TTP or the independent accreditation body itself.

KEY ISSUE

> Procedures to be followed in the event of a dispute with the TTP should be documented.

5.15.11 Storage of information

Where a TTP stores information (such as digital signature keys and encryption keys) in order to provide verification services, secure procedures should be implemented for this storage, in compliance with BIP 0008-1.

Similarly, where the organization stores information (such as responses from the TTP) in order to substantiate verification, secure procedures should be implemented for its storage, in compliance with BIP 0008-1.

KEY ISSUE

> Keys and certificates should be stored in compliance with BIP 0008-1.

5.16 Time considerations

The accuracy of the date and time of a request or of a response may be critical to the organization. Where the accuracy of date and time stamps is critical, an accurate time stamp that can itself be verified should be used.

COMMENT

The time that a verification notice was issued may be key to the determination of a sequence of events. As computer system clocks are frequently inaccurate and not subject to strict control, a verifiable time stamp may need to be added to a verification request and/or response.

Verifiable time can be provided in a number of ways. The organization may decide to implement strict auditable controls over its computer system clocks. This would enable more reliance to be placed on their accuracy. Such clocks may be synchronized using third-party systems.

An externally verifiable time stamp may be considered for specific applications where time is particularly critical. Services are available from third parties, known as Trusted Time (see 5.15.7). This is a time stamp applied to an organization's document, and digitally signed by a TTP. This Trusted Time does not need to be provided by the same TTP that is used for the verification of certificates.

The relevant trusted third-party agreement for the provision of Trusted Time should include the trusted third-party's specifications, interpretations, time zones, formal stamping mechanism and specific liabilities concerned with its time-stamping service.

The TTP should also document how it ensures its Trusted Time is, itself, verified.

INFORMATION

In some cases, the actual time of a verification request is critical. In many cases, however, a more significant issue is that a request is not repudiated because of an erroneous time.

KEY ISSUES

> Where accurate time stamps are required, technology to ensure accurate time recording should be implemented and documented.
> The use of Trusted Time should be considered for time-critical operations.

6 Performance evaluation

6.1 Monitoring, measurement, analysis and evaluation

This section of the Code relates to Clause 9 of BS 10008, 'Performance evaluation'.

In order to be able to demonstrate the effectiveness of the management of the authenticity and integrity of electronic information when linked to electronic identity over time, the system used will need to be monitored and reviewed from time to time.

Thus, audits of the system should be undertaken at planned intervals. Such audits may:

- follow a regular pattern (such as on an annual basis);
- be based on significant changes to the system;
- be as a result of a major system failure; and/or
- be 'without warning'.

6.2 Internal audit

6.2.1 Audit requirements

The essential characteristics of an audit should be borne in mind when developing an audit plan for a procedure or a system. The essential features of an audit are that it:

- has a clearly defined purpose;
- is based on clearly defined and measurable criteria;
- is planned and undertaken competently;
- reaches a fair and objective conclusion; and
- is documented in each of these respects.

The results of an audit will be an audit opinion. Such an opinion should not mislead. The results should include a clear explanation of the purpose of the audit, identify the criteria on which the audit was based and describe the key features of the audit approach (e.g. sources of audit evidence, the extent of reliance on internal controls, use of sampling techniques and/or any significant assumptions). They should also describe the auditor's qualifications for undertaking the work.

KEY ISSUE

> Audits should be defined, planned and undertaken against agreed criteria to enable a suitable audit opinion to be reached.

6.3 Audit planning

The initial stage for the planning of an audit is to determine the purpose for the audit. Such a purpose may be to identify any nonconformance to procedures, or may be to confirm conformance to procedures.

Once the purpose has been established, the scope of the audit should be identified and recorded. Such a scope may encompass the whole organization, a particular part of the organization or a particular process being undertaken within the organization.

It may also be appropriate to define audit criteria. Such a definition will provide a benchmark against which to assess a process, with the objective of establishing the extent to which the audited process conforms to the criteria. Audit criteria take many forms, such as internal standards or procedures, specifications, codes of practice, industry sector standards, or contractual or statutory requirements. Audit criteria may be internally or externally defined, and may be voluntarily, contractually or statutorily imposed. An audit may also aim to provide assurance that the criteria themselves adequately meet the requirements of the stakeholders in the audited process.

In practice, it is generally unnecessary to obtain a very high degree of assurance that audit criteria have been met. It is typically sufficient for the audit to provide 'reasonable' assurance that the activity is free from 'material' error or nonconformance. However, this is not always the case. The evaluation and certification of systems for use in highly secure or safety critical systems is one example of a form of audit that aims to provide a high degree of assurance that audit criteria are being met.

This level of assurance can only be provided on the basis of rigorous and time-consuming testing at commensurate cost.

An audit should be based on a quality plan, incorporating the relevant criteria, to provide a framework within which to work. This helps to ensure that all the activities that are necessary to meet the audit objectives take place in a logical sequence, are allocated to suitably skilled and experienced members of the audit team and are given appropriate weight in relation to their importance in forming an audit opinion. An audit plan also underpins discussions with the audited organization prior to the assignment, supports the agenda for the audit closure meeting and, together with the related audit reports and evidence, forms a permanent record of what has taken place.

KEY ISSUES

> Plan audits against an agreed purpose.
> The level of assurance obtained will depend upon good planning and adequate resource.

6.4 Audit procedures

Where a full system audit is undertaken, there should be procedures that review:

- that all applicable policies are being implemented in an appropriate manner;
- that established procedures are being followed;
- that appropriate technology has been implemented;
- that the technology is configured and maintained in accordance with requirements.

Where partial audits are undertaken, the procedures to be adopted should be such that the scope of the audit is followed.

There should be procedures for the recording of the audit results and of any appropriate analysis. Such results and analysis will lead to the audit opinion.

There should also be a procedure for the retention of evidence that an audit has taken place. It may be beneficial, or even necessary, to provide external bodies with evidence that competently planned and conducted audits have taken place.

KEY ISSUES

> Audits may be undertaken of the whole or of part of a system.
> Retain evidence of audits.

6.5 Selection of auditors

Numerous individuals or bodies undertake audits. Each will have particular reasons for doing so and particular objectives to be met. For example:

- internal auditors provide top management with assurances that policies and procedures are being complied with;
- external auditors are used where an internal audit function is not available, or where an external opinion is required by the organization;
- certification bodies are used to certify against external standards, such as BS EN ISO 9000 and BS ISO/IEC 27001;
- industry regulators such as the Financial Conduct Authority will verify compliance with regulatory requirements;
- government departments will assess and report on compliance with legal requirements, particularly in the accounts and taxes fields;
- customers will monitor the activities of organizations with whom they trade.

Informal audits are also carried out routinely by line managers who review the procedures under their control, and assess these procedures for conformance to policy.

The important issue with the selection of auditors is that the audits are conducted in an objective manner, meet the audit requirements and produce impartial results.

KEY ISSUE

> Select the auditor with care, taking into consideration the required competency and independence.

6.6 Management reviews

6.6.1 General

In order to demonstrate that the system, including the related procedures, is continuing to provide the effective management of attributed electronic documents, regular management reviews should be undertaken. Further, these reviews should be undertaken whenever significant changes to procedures and/or technology are being planned and/or have been implemented.

KEY ISSUE

> Management reviews determine whether the objectives of the system are being met.

6.6.2 Basis for review

Management reviews should be based on:

- general and specific feedback from system users;
- results of the various audits (see 4.5.3);
- records of procedural reviews;
- records of technology modifications.

6.6.3 Results

The management review should be used to assess whether compliance with BS 10008 is maintained. Where a risk is identified that compliance is or may be compromised, then a full review of compliance (see 6.7) should be undertaken.

KEY ISSUE

> Use the results of the management review to determine whether compliance with BS 10008 is maintained.

6.7 Demonstrating compliance

6.7.1 Workbook

The compliance workbook, BIP 0009, may be used to enable a comprehensive assessment to be made of the user's system for conformity to BS 10008, and subsequently to the Code, and to help identify which parts of the Code are relevant.

Compliance with the Code should be claimed only if all recommendations, as stated in the workbook, have been met, or justifications for any non-applicable recommendations have been documented. Compliance with the Code should be claimed via an authorized statement, examples of which are shown in 6.7.2.

Electronic identity management systems should be audited on a regular basis to ensure that the provisions of the Code are being met and that the approved procedures are being adhered to. This audit should review audit trail data that are produced on a regular basis for evidence of ongoing, continuous compliance.

The person identified in 2.2.2 as being responsible for maintaining compliance with the Code should review the results of each audit and document/implement a plan to address any non-compliances, which should be re-audited.

A record of compliance with the Code should be maintained, as part of the audit trail. This record should include details of which recommendations are not considered relevant and justifications for these decisions.

Where compliance with previous editions of the Code has been claimed, copies of those editions should be retained as part of the compliance audit trail.

Where any change is made to the electronic identity management systems, or to relevant procedures, that affects compliance with the Code, a new audit of compliance should be undertaken.

Auditing may be carried out by authorized and trained in-house staff or by suitable third parties.

KEY ISSUES

> Use the compliance workbook (BIP 0009) to audit and document compliance with the Code.
> Re-audit on a regular basis, and during major system changes.

6.7.2 Statement of compliance

6.7.2.1 General

Compliance with the Code should be claimed using statements, which differ depending upon whether:

- the end user organization is claiming compliance;
- the system supplier is claiming that a system can be used in a compliant manner; or
- a third party, acting as auditor, is confirming a compliance status.

Recommended text is given below for use in compliance statements. Alternative text may be used, but legal advice should be sought to ensure its suitability.

6.7.2.2 End user organizations

Individuals who, or organizations that, conduct audits of their own electronic identity management systems may certify compliance via the following statement:

> '[insert name of organization] confirms that the [insert name or other identification for the system] electronic identity management system is operated in compliance with BS 10008:2014.'

The statement should be signed by an officer of the organization, stating his or her position.

NOTE: The policy document should identify the individual or position within the organization authorized to sign statements of compliance with the Code (see Chapter 4).

6.7.2.3 System integrators and developers

Individuals who, or organizations that, integrate/develop/supply electronic identity management systems may certify that their systems may be used in a compliant manner via the following statement:

> 'The [insert name or other identification for the system] electronic identity management system supplied by [insert name of integrator/developer/supplier] provides all facilities necessary for a user of this system for implementation in compliance with BS 10008:2014.'

The statement should be signed by an officer of the supplier organization, stating his or her position.

6.7.2.4 System auditors

Individuals who, or organizations that, conduct audits of electronic identity management systems may certify compliance via the following statement:

> '[insert name of auditing organization or individual] has assessed the [insert name or other identification for the system] electronic identity management system operated by [insert name of organization] for compliance with BS 10008:2014 and hereby certifies its compliance.'

The statement should be signed by an officer of the auditing organization, stating his or her position.

KEY ISSUE

> Claim compliance using an authorized statement.

6.7.3 System audit trail

The system audit trail should store details of significant events, primarily to enable users to determine the status of the system at a relevant time in the past. There should be sufficient information to enable the user to determine whether the system was 'working normally' when a particular event occurred.

Where information has been converted from one format to another, as part of the electronic identity management system, details of the conversion processes should be stored in the audit trail.

KEY ISSUES

- > System audit trails should be able to demonstrate 'proper working' of the system.
- > They should also be able to demonstrate the successful completion of format conversion processes.

7 Improvement

7.1 General

This section of the Code relates to Clause 10 of BS 10008, 'Improvement'.

It is important to improve procedures and systems wherever appropriate. Such improvements may be to ensure that an identified issue is resolved without compromise to attributed electronic documents, and that the risk of a reappearance of the issue is minimized. The improvements may also relate to updated techniques and/or technology that will improve performance or reduce operational costs.

Any proposed improvement in procedures and/or technology should be assessed prior to its implementation to ensure that compliance with the electronic identity and information security policies is not compromised.

Where major changes are implemented, an audit trail of the change management procedure should be produced and retained in line with the retention schedule. This audit should be completed as soon as possible after changes have been made.

KEY ISSUE

> Ensure that procedures and systems are being maintained and improved by assessing the conclusions of audits.

7.2 Preventive and corrective actions

7.2.1 General

Any proposed improvement in procedures and/or technology should be assessed prior to its implementation to ensure that compliance with the identity management and information security policies are not compromised.

Where major changes are implemented, an audit trail of the change management procedure should be produced and retained in line with the retention schedule. This audit should be completed as soon as possible after changes have been made.

7.2.2 Preventive

In order to reduce the risk of nonconformities in relation to compliance with the electronic identity and information security policies, preventive actions should be undertaken.

In order to identify any nonconformity at an early stage, the audit procedures identified in 6.4 should be followed at regular intervals.

Where a nonconformity is found, the cause of the nonconformity should be identified. An evaluation of the cause should then be completed, to identify the likelihood of the nonconformity reoccurring.

Where the identified risk is significant, procedures and/or technology should be reviewed to identify ways of reducing this risk. Any identified actions from this review should be implemented.

The results of the review and details of the preventive actions taken should be documented and retained in accordance with the retention schedule.

KEY ISSUE

> Take preventive action to reduce the risk of nonconformities occurring.

7.2.3 Corrective

From time to time, issues will arise that will or may result in a nonconformity occurring. There may, for example, be an actual or a suspected security breach. In these instances, corrective action should be taken to:

- assess and document any compromise to the authenticity, integrity and/or availability of the information affected;
- identify and action procedures for recovery from any compromise (maybe by a restore from backup);
- reassess the attributed electronic documents once recovery procedures have been implemented;
- document any residual issues found by the reassessment;
- review the actions taken and identify (see 7.2.2) actions to be taken to prevent a reoccurrence of the issue.

KEY ISSUE

> Take corrective action to recover from nonconformities.

7.3 Continual improvement

7.3.1 General

There should be a mechanism for considering and acting on the findings of an audit. Although the auditor may recommend the general nature of any remedial action to correct problems uncovered by the audit, and may subsequently undertake further work to assess the extent to which remedial action has been successful, it is not the auditor's role to specify or impose particular solutions.

Organizations should review the results of all forms of audits (see 6.4) with an objective of continually improving the system. Such improvements can take many forms:

- system efficiency;
- system effectiveness;
- ease of operation;
- speed of operation;
- reduced risk of compromise to attributed electronic documents;
- reduced risk of procedures not being followed.

KEY ISSUE

> Continual improvement should be an objective of the system.

7.3.2 Training

In order to be able to ensure that the procedures detailed in the procedures manual (see 4.5.2.3) are followed, staff need to be aware of them and have the ability to follow them. This situation is frequently achieved by training, either by specific courses or during day-to-day working.

Training should be given to staff prior to them being given access to the appropriate parts of the system. Ongoing training should then be used to identify improvements within the system.

EXAMPLE

After specific training, the organization's group audit function took on the role of checking that procedures for the operation of all aspects of the electronic identity management systems were being followed. Checks were made at the same time as other audit checks were being made, including spot checks and scheduled reviews.

KEY ISSUE

> Training is needed to ensure that all staff who have access to the electronic identity management systems adhere to agreed procedures.

Annex A Example electronic identity management policy statement

This annex contains an example 'electronic identity management policy statement'. It can be used as a draft upon which an organization's policy can be based.

XYZABC Limited

ABC project

Policy document for compliance with the requirements of BS 10008:2014, *Specification: Evidential weight and legal admissibility of electronic information*.

Approved by:
Name:
Position:
Date:

1. Scope

This document covers the electronic identity management policies for associating electronic identity with electronic documents implemented within the XYZABC Limited electronic information systems. These systems identify individuals or processes actioning documents and separately assert XYZABC Limited's intellectual property rights to documents and other digital assets.

The following systems are used to identify individuals:

- HIJ electronic transfer system;
- KLM internet web service;
- PQR automated reporting system;
- STU electronic records management system;
- XYZABC Limited email system.

These electronic information systems are described in a system description manual (Ref: SD02). Procedures for the use of the systems are described in a procedures manual (Ref: PM02).

This policy conforms to the requirements of BS 10008:2014, *Specification: Evidential weight and legal admissibility of electronic information*.

2. Information covered

Identity and digital rights information covered by this policy document relates to those documents used in relation to all aspects of electronic transfers and document retention for XYZABC Limited. Documents included within the scope of this policy cover identity and digital rights associated with documents by XYZABC Limited and other parties.

XYZABC Limited does not operate an information classification system, as all information is regarded as having the same security level.

3. Identity attributes formats

All identity and digital rights information is associated with specific documents and is held in formats appropriate to the application.

4. Standards

All identity and digital rights information within XYZABC Limited is managed in compliance with BS 10008:2014, together with any referenced national and/or international standards.

All identity information transferred within, to or from XYZABC Limited is in documents that are transferred in compliance with BS 10008:2014; all identity information in documents within XYZABC Limited is stored in compliance with BS 10008:2014.

5. Identity and digital rights information

5.1 General

All systems used within XYZABC Limited are the property of XYZABC Limited and are provided to help meet the business aims and responsibilities of XYZABC Limited; staff, contractors and others utilizing these systems have no expectation of privacy relating to their use of these systems.

5.2 Identity

This section deals with electronic documents with identity associated with the electronic transfer system.

For each document type within each system identified, the following will be considered and will cover the identity of XYZABC staff and other parties, as well as appropriate XYZABC systems and processes:

- identity formats;
- applying identity to documents;
- issuing and using tokens and credentials used to identify individuals, processes or systems, for example digital certificates and cryptographic keys;
- verification processes for documents with identity associated;
- ensuring that identity is not falsely attributed or claimed;
- the use and responsibilities of third-party service providers.

In all cases where a document has identity associated with it, it will be retained, and at the appropriate time destroyed, in compliance with BS 10008:2014.

5.3 Digital rights

This section deals with the digital rights of information held by or communicated with XYZABC on a regular or an ad hoc basis. This includes the following systems:

- KLM internet web service;
- STU electronic records management system;
- XYZABC Limited email system.

XYZABC will not abuse and will respect the digital rights of others vested in or associated with documents used by XYZABC.

All XYZABC documents used or transferred outside XYZABC will be marked with appropriate copyright and other digital rights attributes. This will, for specified document types, include protection mechanisms to ensure that only authorized parties within and outside XYZABC have access to controlled document content.

Special consideration must be given to person-to-person email. Messages sent or received by email can be highly effective, if properly used, or highly damaging, if improperly used. Messages sent by XYZABC are the copyright of XYZABC, unless specific content within them is clearly shown to be the copyright of a third party. Email received by XYZABC remains the copyright of the sender unless specifically indicated otherwise.

Guidelines for the proper use of email, and sanctions that will be imposed for improper use, are detailed in the internet acceptable use policy (Ref: IAUP01). These guidelines include details of copyright, ownership and monitoring of all emails.

6. Responsibilities

This policy document should be reviewed annually under the control of the Company Secretary. Where changes are agreed, they are to be implemented using the change control procedures (Ref: CC01).

This policy, plus any revisions, should be approved by the Board of Directors of XYZABC Limited prior to implementation.

The maintenance of compliance with BS 10008:2014 is the responsibility of the Head of Internal Audit.

7. Legal advice sought

XYZABC Limited has sought and obtained agreement for this policy.

8. Duty of care

XYZABC Limited has a duty to keep secure and accurate original documentation, or authentic copies of them. This is achieved by:

- implementing this policy document;
- implementing an information security policy;
- ensuring that only trained staff have access to the system;
- ensuring that acceptable quality control procedures are implemented; and
- ensuring that XYZABC Limited's legal advisers are consulted and appropriate actions are taken.

Annex B References

BSI publications

British Standards Institution, London. BSI Publications are available from Customer Services, Sales Department, 389 Chiswick High Road, London W4 4AL. Tel: 020-8996-9001; Fax: 020-8996-7001

Standards

BS 10008:2014, *Evidential weight and legal admissibility of electronic information — Specification*

BS EN ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

BS EN ISO 9001:2008, *Quality management systems — Requirements*

BS ISO/IEC 9594-8:2014, *Information technology — Open Systems Interconnection — The Directory — Public-key and attribute certificate frameworks*

BS ISO/IEC 10118-3:2004, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

BS ISO/IEC 21000-5:2004, *Information technology — Multimedia framework (MPEG-21) — Rights Expression Language*

BS ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

BS ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security management*

BS ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

BS ISO 31000:2009, *Risk management — Principles and guidelines*

Guidance documents

BIP 0008-1 (2014), *Evidential weight and legal admissibility of information stored electronically — Code of practice for the implementation of BS 10008*

BIP 0008-2 (2014), *Evidential weight and legal admissibility of information transferred electronically — Code of practice for the implementation of BS 10008*

BIP 0009 (2014), *Evidential weight and legal admissibility of electronic information — Compliance workbook for use with BS 10008*

Other publications

Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce (1996), Chicago: American Bar Association (ABA). Available at: www.abanet.org/scitech/ec/isc/dsgfree.html

ANSI X9.31:1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* New York: American National Standards Institute (ANSI)

ANSI X9.62:2005, *Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA),* New York: American National Standards Institute (ANSI)

Berne Convention for the Protection of Literary and Artistic Works. Paris Act of July 24, 1971, as amended on September 28, 1979. Available at: www.wipo.int/treaties/en/ip/berne/pdf/trtdocs_wo001.pdf

ETSISR 002 176 V1.1.1 (2003), *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures*, Sophia-Antipolis: European Telecommunications Standards Institute (ETSI). Available at: www.etsi.org/technologies-clusters/technologies/security/electronic-signature

ETSI TS 102 023 V1.2.2 (2008), *Electronic Signatures and Infrastructures (ESI); Policy Requirements for Time-Stamping Authorities*, Sophia Antipolis: European Telecommunications Standards Institute (ETSI). Available at: www.etsi.org

Federal Information Processing Standards Publication (FIPS PUB) 180-4 (2012), *Secure Hash Standard (SHS),* Gaithersburg: National Institute of Standards and Technology (NIST). Available at: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

The UK Corporate Governance Code (formerly known as *The Combined Code)* (2014) London: The Financial Reporting Council Limited. Available at: www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-2014.pdf

The UK Approach to Corporate Governance (2010) London: The Financial Reporting Council Limited. Available at: www.frc.org.uk/Our-Work/Publications/Corporate-Governance/The-UK-Approach-to-Corporate-Governance.pdf

Internal Control: Revised Guidance for Directors on the Combined Code (2005), London: The Financial Reporting Council. Available at: www.frc.org.uk/getattachment/5e4d12e4-a94f-4186-9d6f-19e17aeb5351/Turnbull-guidance-October-2005.aspx

Regulation of Investigatory Powers Act 2000, 2000 Chapter 23, London: http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

Good Practice Guide: Organisation Identity (GPG 46) (2013), London: CESG, National Technical Authority for Information Assurance and the Cabinet Office. Available at: www.gov.uk/government/publications/identity-assurance-organisation-identity

Identity Proofing and Verification of an Individual (GPG 45) (2013), London: CESG, National Technical Authority for Information Assurance and the Cabinet Office. Available at: www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

Good Practice Guide: Authentication Credentials in Support of HMG Online Services (GBG 44) Available at: www.gov.uk/government/publications/authentication-credentials-for-online-government-services

XML Signature Syntax and Processing (Second Edition) (2008), World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF). Available at: www.w3.org/TR/xmldsig-core/

Office of the e-Envoy (England), *Registration and Authentication – e-Government Strategy Framework Policy and Guidelines*, Version 3.0, London, HMSO (2002).

RFC 3161 (2001) *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, Internet Engineering Task Force (IETF). Available at: www.ietf.org/rfc/rfc3161.txt?number=3161

RFC 3851 (2004) *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*, Internet Engineering Task Force (IETF). Available at: www.ietf.org/rfc/rfc3851.txt?number=3851

Guidance for Assessments (tSi0250 Issue 2.03) (2004) London, tScheme Limited. Available at: www.tScheme.org/

tScheme and Confidence in Online Identity, London: tScheme Limited (2004). Available at: www.tScheme.org/

The tScheme Guide to Securing Electronic Transactions (tSi0256 1) (2002) London, tScheme Limited. Full and shortened versions available at: www.tscheme.org/

Approval Profiles, London: tScheme Limited. Available at: www.tscheme.org/profiles/index_digest3.html

USA (1998) Identity Theft and Assumption Deterrence Act of 1998 (18 USC 1028), as amended by Public Law 105–318—Oct. 30, 1998. 112 Stat. 3007. Available at: www.ftc.gov/node/119459

USA (2002) Sarbanes—Oxley Act of 2002
Available at: http://www.sec.gov/about/laws/soa2002.pdf

Evidential weight and legal admissibility of linking electronic identity to information

Code of practice for the implementation of BS 10008

Evidential weight and legal admissibility of linking electronic identity to information – Code of practice for the implementation of BS 10008 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.

Now in its fifth edition, the book details operational procedures and technology requirements for these equivalent methods, providing essential good practice guidance for the use of electronic identity systems, covering the following key areas:

- sender and recipient identity verification;
- evidentially provable electronic signature;
- linking of identity of copyright ownership to an electronic document.

This fifth edition is technically similar to the fourth edition, but has been restructured in recognition of the publication of BS 10008:2014, and can be considered to be a guide to the implementation of the standard in relation to linking electronic identity to information.

This publication is the third part of BIP 0008. The other two parts are:
BIP 0008-1 (2014), *Evidential weight and legal admissibility of information stored electronically – Code of practice for the implementation of BS 10008;*
BIP 0008-2 (2014), *Evidential weight and legal admissibility of information transferred electronically – Code of practice for the implementation of BS 10008.*

This book provides guidance on how your organization can:

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

Peter Howes

Peter Howes is Director and Principal Consultant for Group 5 Training Limited and is a specialist in the practical issues of legal and regulatory compliance, governance, electronic communications and information security, with over 40 years' relevant experience in the business application of information systems. For the last 20 years, Peter has worked with BSI to develop the full range of evidential weight and legal admissibility publications and has delivered a wide range of workshops on evidential weight as well as email records management, email and the law, information security and the law with BSI.

Alan Shipman

Alan Shipman is Managing Director and Principal Consultant for Group 5 Training Limited. He has been involved in Document Imaging Standards for over 20 years, specializing in user aspects. Alan is Chairman of the BSI Document Imaging Applications committee, convenor of the ISO Document Imaging Quality sub-committee and a member of the UKAIIM Standards Committee. Alan has presented BSI Training Workshops on the practical implementation of BIP 0008, as well as speaking on the subject at events in the information management, archives and records management fields and also at industry specific events in educational, engineering, health care, financial, legal, local government and system supplier fields.

bsi.

BSI Group Headquarters
389 Chiswick High Road
London W4 4AL
www.bsigroup.com

BSI order ref: BIP 0008/3

9 780580 856785

The British Standards Institution is incorporated by Royal Charter