ASIC

Australian Securities & Investments Commission

EDGE

ELECTRONIC LODGEMENT SYSTEM

Digital Signature SPECIFICATION

Version 1.02

27th February 2004

Notice To Readers

This specification is current at the latest date shown in the Amendment History, but it may be amended at any time without prior notice. Only developers of packages currently registered for the Electronic Company Registrations component of EDGE lodgement will be notified of changes.

ASIC is not responsible for the quality or merchantability of software developed on the basis of this specification, nor is it responsible for any application packages developed by third parties to prepare and lodge documents onto the EDGE system. ASIC does not support such software in any form.

Contents

1. INTRODUCTION

1.1. Who should read this document

This document is written for persons developing software which creates electronic documents intended for transmission to ASIC's EDGE system.

This document covers the requirements for digital signature of documents and transmissions.

This document may be of interest to persons investigating problems with such software, persons using such software and persons developing other Corporations Law related software.

1.2. The purpose of this document

This document describes the use of digital signatures with ASIC's EDGE electronic lodgement system.. It must be read in conjunction with the other EDGE documentation listed in 1.3 below, in particular the EDGE messages specification. It describes the requirements for:

- the business rationale
- the technical specifications

1.3. Other relevant documentation

EDGE specifications are available for download from **"http://www.asic.gov.au/api".**

Publicly available documentation of ASIC's EDGE electronic lodgement system is listed in the Document Summary document in these specifications.

ASIC may prepare other specifications and directions from time to time. They will be distributed to registered software developers.

1.4. Where to get help

Refer to the Documentation Summary specification

2. BUSINESS RATIONALE FOR USE

2.1. Why are digital signatures being used

Document signature

To provide an appropriate level of authentication for electronically lodged documents, ASIC will utilise digital signatures generated using the private key associated with an X.509 certificate issued by an approved certification authority.

Digital signatures will be mandated for certain company registration messages.

Digital signatures may optionally be used on other documents, provided that the signatory possesses a suitable X.509 certificate and the agents trading agreement authorises its use.

Transmission signature

Company registration documents are high value documents whose lodgement incurs a debt from the lodging party to ASIC. To provide a level of authentication and security commensurate with the transaction values that may be involved, such transmissions must be digitally signed.

Additionally, the use of the Internet requires additional measures to ensure message integrity. All transmissions using the Internet which contain documents requiring digital signature as described above, must also be digitally signed. Transmissions that do not contain such documents do not require a digital signature. Where the transmission does not contain digital signature, the SSL session encapsulation of authentication and transmission is taken to provide sufficient message integrity.

2.2. When are digital signatures to be used

The EDGE Electronic Lodgement Protocol, available from ASIC's home page at http://www.asic.gov.au, determines the conditions of use of digital signatures.

In summary, at time of writing

- Documents **must** be digitally signed when the relevant message specification indicates that the digital signature segments (ZXI/ZXS) are mandatory. Mandatory digital signatures apply to company registration documents.

- Other documents **may** be digitally signed.

- Transmissions **must** be signed if they contain company registration messages.

2.3. Signing documents

Company registration documents must be digitally signed by the applicant.

Where a company officer is required to sign register documents, and the officer has obtained an approved X.509 certificate, then the register document may be digitally signed.

2.4. Signing transmissions

Transmissions must be digitally signed if they contain documents which themselves require digital signatures, to

- provide message integrity for messages transmitted over the internet
- for company registration messages, to acknowledge agent responsibility for payment of statutory charges for company registration messages included in the transmission

2.5. Certification Authorities

ASIC will recognise certificates issued by one or more third party commercial certification authorities. ASIC intends to recognise certification authorities that meet the whole of government requirements defined by the GateKeeper project.

The EDGE Electronic Lodgement Protocol, available from ASIC's home page at http://www.asic.gov.au, provides details of Certification Authorities whose certificates may be used with the EDGE system.

Chapter 4 provides further details.

2.6. Authorising certificates

This section does not apply to agents who have do not intend to lodge company registration documents". These non-ECR agents may use the EIS service without client certificates.

In the current implementation of digital signatures, ASIC will operate a closed system with its registered agents. A trading agreement will be entered into before lodgment is permitted.

Within this closed environment, agents will need to set authorities attached to certificates directly with ASIC using EDGE messages, in addition to any revocation which the agent may perform to their certification authority. Changes to certificate authorities, and notification of new certificates, are made using an RA53 message, signed by an already authorised certificate

On first entering a trading agreement with ASIC to lodge company registration transmissions, an agent will be provided with a single use PIN number to authorise the first certificate. This PIN must be sent to ASIC in a transmission signed using certificate to be initially authorised. This is called a "self authorised" message. This method will also be used if a new initial certificate needs to be authorised. This might occur if, for example, the only authorised certificate is lost.

Certificates may be authorised at two levels

- transmission signature, which includes authorising the creation of a debt by the agent to ASIC for statutory fees payable on company registration messages included in a transmission
- document signature, as an applicant or a company officer

A certificate may be authorised at both levels.

2.7. Security of private keys

The terms and conditions for issue of X.509 certificates generally place certain responsibilities on the user of the certificate to secure the private key.

The technology used to store the private key has a major impact on the level of security provided. In particular, storage of private keys on computer hard disks is considered to provide only a very low level of security and does not meet the GateKeeper requirements.

Software developers are referred to various Internet information sources for details on the ease with which keys stored on hard disk can be uploaded and mis-used.

GateKeeper recognises storage on floppy diskette, PCMCIA cards, removable disks and smart cards.

2.8. Other security services for the Internet

Digital signature of transmissions will provide a high level of message integrity and user authentication for EDGE lodgements both over the Austpac X.25 service and over the Internet.

For Internet traffic, ASIC will also run encrypted traffic to provide confidentiality of traffic content. This will be achieved by using SSL-3 encryption between server and client using 128bit encryption keys. The SSL-3 sessions will not utilise client authentication using client X.509 certificates. This will be provided by the encrypted user id/password pair, plus the digital signature of transmissions, for transmissions containing registration documents.

2.9. Gatekeeper specifications

At time of writing, the GateKeeper report is available from the National Office of the Information Economy at http://www.noie.gov.au

3. TECHNICAL SPECIFICATION

3.1. Base-64 encoding

The EDGE message definition language supports a base64 encode element. This must be encoded according to RFC1421. In creating EDGE segments, the newline character defined to delimit base64 also serves as the EDGE segment delimiter.

3.2. Encoding a certificate

Before being used to sign ASIC messages, certificates must be authorised to ASIC using an RA53 message. The certificate must be base64 encoded, then assembled into a set of ZXC segments as defined in this message.

3.3. Encoding a signature

Digital signatures are appended to EDGE messages as a ZXI segment to identify the certificate containing the public key, and a set of ZXS segments containing the base64 encoded signature.

3.4. Signing a document

The message digest on an EDGE document must be hashed over the complete data component of the message, commencing with the ZHD header segment, and ending with the new-line which delimits the ZTR trailer segment.

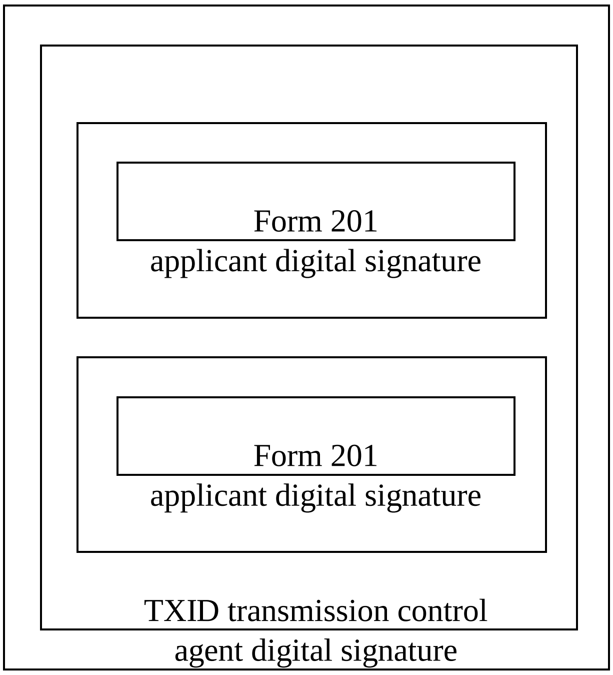
If the document is signed using a certificate which has not been pre-authorised to ASIC using an RA53 (in this specification, referred to as self authorising), the base64 encoded certificate is assembled as ZXC segments and appended to message.

Attention: In the current implementation of EDGE, the only messages which may be self authorised are RA53 messages which contain an ASIC issued single use PIN to allocate authorities to the certificate.

A ZXI segment is then appended to the message to identify the X.509 certificate associated with the private key being used to sign the document and to advise algoriths used.

The digital signature is then calculated, encoded to base64 according to RFC1421, converted to a set of ZXS segments according to EDGE requirements and appended to the message.

3.5. Signing a transmission


Form 201
applicant digital signature
Form 201
applicant digital signature
TXID transmission control
agent digital signature

All documents (including digital signature segments if appropriate) to be transmitted are assembled into a single message and the TXID file is appended.

The message digest must be hashed over the assembled message, starting at the start of the first ZHD segment, and ending with the newline of the ZTR segment of the TXID.

If the transmission is signed using a certificate which has not been pre-authorised to ASIC using an RA53 (in this specification, referred to as self authorising), the base64 encoded certificate is assembled as ZXC segments and appended to message.

Attention: In the current implementation of EDGE, the only transmissions which may be self authorised are those containing a single RA53 message which contains an ASIC issued single use PIN to allocate authorities to the certificate.

A ZXI segment is then appended to the message to identify the X.509 certificate associated with the private key being used to sign the transmission.

The digital signature is then calculated, encoded to base64 according to RFC1421, converted to a set of ZXS egments according to EDGE requirements and appended to the message.

3.6. Self Authorised Transmissions

RA53s

Because certificates are normally pre-authorised to ASIC using a signed RA53 message, it is not normally necessary to transmit the X.509 certificate as part of the digital signature group.

However, this is not the case when an agent first joins the EDGE Company Registrations system, or in re-establishing authorities if the only authorised certificate is lost. In these cases, it is necessary to use a self authorised transmission of an RA53 message which in turn contains a single use ASIC issued PIN.

A self authorised transmission must contain one and only one RA53 message, which in turn must contain the ASIC issued PIN. The ZXC segments within the digital signature group of the RA53 must contain the certificate used to sign the document. This certificate must match the certificate whose authorities are being set by the RA53. Similarly, the transmission must be signed by this certificate and the signature group of the TXID must contain this certificate.

Future Use

As the use of digital signatures developes and the structures which support levels of trust in these signatures matures, ASIC may accept messages signed using certificates which have not been pre-authorised using an RA53 message.

The structure of the digital signature group will allow certificates to be transported as part of these messages

3.7. Useful libraries

OpenSSL (formerly SSLeay)

OpenSSL is a widely used software package which provides comprehensive SSL and X.509 cryptographic services. The package is extremely popular with developers and is incorporated in many commercial packages. Its popularity stems from:

- it is comprehensive and of high quality.
- it was developed outside the US, in Australia, and so is not subject to the US laws prohibiting export of strong cryptographic software which affect much of the world’s commercial cryptographic libraries.
- the package is available in source form, so patches can be quickly applied.
- it is free. This helps to guarantee availability and ensures good Internet-based support.

The package is available via the Internet from:

ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL

A search in any of the major Internet search engines on the keyword “ssleay” will quickly reveal many mirror sites and related resources.

3.8. Test keys for software developers

ASIC can provide test certificates and private keys for developers of EDGE software.

Software developers who intend to provide digital signature capability should contact the EDGE systems team.

3.9. Implications for X.25 users

EDGE messages are defined to use a restricted character set. However, use of certain characters such as the carriage return has historically been tolerated to retain DOS compatability.

Such characters may be removed by transmission protocols such as Zmodem in ASCII mode. As the digital signature digest would have been calculated to include those characters, the signature check would fail and EDGE would reject the document.

Developers should restrict their messages to the defined character set.

As a fall back, it is possible to force Zmodem binary transfer, although ASIC does not recommend this approach and does not guarantee future compatability.

3.10 Format of Distinguished Names

3.10.1 Overview

Distinguished names in X.509 certificates are represented internally using ASN1 Abstract Syntax Notation One), but there is no definitive format for external string representations. ECR follows the SSLeay (now OpenSSL) usage, which follows Internet RFC1779.

3.10.2 Rules

Rules are as follows:

- distinguished names (DN's) must be shown as a set of key/attribute pairs separated by "/" characters.
- attribute values must be extracted from the cerificate, in the same order as they appear in the certificate.
- The DN must include all attributes contained in the certificate for the DN.

- Each key/attribute pair must be of the form: key=attribute where "key" can be one of the names shown on the LEFT side of the RFC1779 Keyword/Attribute table below. These keywords must be in UPPER CASE.

- if certificates issued by suppliers accepted by ASIC for ECR contain elements prefixed by keywords other that those in the table, then those keywords must be rendered as they appear in the certificate, but in UPPER CASE

- Key/attribute pairs must be separated by "/" characters. This follows the SLeay/OpenSSL usage when displaying subject names, and follows the OSF Syntax, as referred to by this phrase in RFC 1779 :

  > "The OSF Syntax may be more appropriate for some system oriented uses. (The OSF Syntax uses "/" as a separator, and forms names in a manner intended to resemble UNIX filenames)."

- Attribute values extracted from certificates must be shown EXACTLY as they occur in the certificate, hence they are case sensitive.

3.10.3 RFC1779 Keyword/Attribute table

Key	Attribute (X.520 keys)
CN	CommonName
L	LocalityName
ST	StateOrProvinceName
O	OrganizationName
OU	OrganizationalUnitName
C	OrganizationalUnitName
STREET	OrganizationalUnitName

3.10.4 Examples

These are valid for ECR:

/C=au/O=KeyPOST Test CA

/C=AU/O=ECR Test CA

These are NOT valid for ECR:

/c=au/O=KeyPOST Test CA (key "c" is in lower case, must be upper)

/C=AU/O=KeyPOST Test CA (in the circumstance where the actual certificate shows lower case "au" as the country, so it must appear here in lower case.)

3.11 Error Codes for ECR Validation Signature Errors

Where digital signatures fail verification, a message similar to these two messages will appear in the validation report:

X027 Digital signature verify failed, X509 verify retcode=37

X028 BCHN signature verify failed, X509 verify retcode=37

The item of interest in these messages is the **retcode**. Most return codes indicate internal errors and are not visible to clients, i.e. they do not appear in validation reports. The values and meanings of those codes likely to appear in validation reports are:

Retcode value	Meaning	Explanation and Solutions
25	No signature found	Decode software could not find a signature - check that a signature was appended and it was in the correct place.
26	Invalid ZXI	The ZXI segment was not correctly formed.
27	Invalid ZXI issuer	The issuer DN found in a ZXI segment did not match any of the DNs of issuers accepted by ASIC for ECR.
28	Invalid ZXI hashcode	The code indicating the hashcode used in producing the message digest is not one supported by ECR. MD5, SHA1 and SHA-1 are supported.
29	Invalid ZXI crypt	The code indicating the encryption algorithm used for the signature is not one supported by ECR. RSA is supported.
35	X509 read error	The decode software could not read the X509 certificate, probably indicating the certificate is corrupt, not a certificate, or incorrectly represented in the message. Review method used to encode the certificate.
37	Signature verify failed	The decode software signature verification processing indicated that the signature was not correct. This can be because the signature was not that of the data sent e.g. the wrong data buffer was signed, or it can be because the signature data structure is not a valid digital signature. This usually indicates signature software failure.

The most common causes of signature errors are:

- operator does not insert smartcard in reader, but software does not detect error. This often results in signatures with no data in the ZXI segments.

- client software does not sign the exact data required to be signed. Document signatures must sign the data from the start of the ZHD header segment up to and including the linefeed character at the end of the ZTR trailer segment. BCHN (i.e. message) signatures must sign all data from the start of the message to the linefeed character at the end of the TXID ZTR trailer segment in the TXID appended to the BCHN.

- client software appends carriage returns or other data after signature. ECR must receive exactly the bit-string signed, no more, no less, or the signature verification will fail.

- client software generating the signature fails, due to incorrect version, incorrect configuration, or bugs. If this software is third-party, which most are, then consult your vendor software support.

Note that signature verification errors should never occur if the client software correctly performs a signature verification prior to sending the message to ECR. In practice this can be difficult to achieve, because often if errors occur the verification processing repeats the error in the original signature processing. Nevertheless software developers are encouraged to build in independent signature verification where this is possible, so that invalid signatures do not leave the client machine.

4. Recognition for EDGE lodgement

4.1. Certification authorities

- EDGE will recognise private/public key pairs and X.509 certificates issued by the certification authorities specified in the EDGE Electronic Lodgement Protocol, available from the ASIC Home Page at http://www.asic.gov.au

4.2. Key storage media

EDGE will recognise the following key storage media

- crypto smart card (strongly recommended)
- memory smart card
- floppy diskette
- PCMCIA card
- removable hard disk

Appendix A - Amendment History

Version 00.10

Released to software suppliers as a draft for information on 31/03/98.

Version 00.90

Released to software suppliers as a draft on 30/06/98.

Version 00.95

Released to software suppliers as a draft on 04/09/98.

Change 2.1, 2.3, 2.6, 3.4, 3.5
Add 3.6

Version 01.00

Released to software suppliers on 09/10/98.

Initial production release with no changes from the version 0.95 draft.

Version 01.01

Released to software suppliers on 12th November 2001

4.1 – refer to the EDGE protocol for supported certification authorities.

Added 3.10 Format of Distinguished Names. This section provides detailed rules and examples for construction of Distinguished Names in ECR messages.

Added 3.11 Error Codes for ECR Validation Signature Errors. This section provides error codes, causes and explanations for all errors that clients and software developers are likely to see. A guide to common signature errors is also included.

Version 01.02

Released to software suppliers on 27th February 2004

Changes to allow lodgement of documents other than Electronic Company Registration documents via the Edge Internet Interface without the need for digital signatures:

Section 2.1, para headed "Transmission signature", change the last sentence to read:

"All transmissions using the Internet which contain documents requiring digital signature as described above, must also be digitally signed. Transmissions which do not contain such documents do not require a digital signature. Where the transmission does not contain digital signature, the SSL session encapsulation of authentication and transmission is taken to provide sufficient message integrity."

Section 2.2, first para, third dot point, remove:

", or if they are transmitted over the Internet".

Section 2.4, first line, insert between "signed" and "to":

"if they contain documents which themselves require digital signatures".

Section 2.6, insert before the first para:

"This section does not apply to agents who have do not intend to lodge company registration documents". These non-ECR agents may use the EIS service without client certificates."

Section 2.8 at the end where it says "plus the digital signature of transmissions", add:

", for transmissions containing registration documents".

Reelased to software developers on 26 February 2014

Section 3.11 – Retcode 28, add reference to SHA1