



The National Office for the
INFORMATION ECONOMY

Australian Business Number Digital Signature Certificate (ABN-DSC)

Implementation of the ABN Private Extension

Version 1.3

November 2001

National Office for the Information Economy

This work is copyright. The Commonwealth grants a royalty-free, irrevocable, world-wide, perpetual, non-exclusive licence, including the right to sub-licence, to reproduce this work for the purpose of gaining accreditation under the Gatekeeper strategy. Apart from this purpose and any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without the prior written permission from the National Office for the Information Economy. Requests and enquiries concerning reproduction rights should be addressed to:

*Manager
Authentication Implementation
Government Online
National Office for the Information Economy
Level 3 Centenary House
19 National Circuit
BARTON ACT 2600*

*Phone: (02) 6271 1531
Email: doug.conn@noie.gov.au*

Table of Contents

Table of Contents	3
1. Introduction	4
2. Placing the ABN in its own private extension	4
3. OID for the ABN Extension	4
4. Extension structure	5
Figure 1 - ASN.1 syntax for ABN Private Extension.....	5
Figure 2 - Extension structure for ABN-DSC	5
5. Sample ABN-DSC Authentication Certificate	5
Annex A - ASN.1 Module using 1988 Syntax	10

1. Introduction

This paper should be read in conjunction with the ABN-DSC Broad Specifications, Version 3.5, issued by NOIE in November 2001 and available on the NOIE website at ([http://www.govonline.gov.au/projects/publickey/ABN-DSC Broad Specs-FINAL.pdf](http://www.govonline.gov.au/projects/publickey/ABN-DSC%20Broad%20Specs-FINAL.pdf)).

The inclusion of the ABN of the subject in the ABN-DSC class of certificate provides an important characteristic of the certificate in its use to identify a business entity.

A number of options for locating the ABN in the certificate were considered. The most suitable location for this identifier was deemed to be in a private certificate extension.

Further work has now been undertaken to define the structure and syntax for the extension. Again a number of options were considered and discussed with key stakeholders.

2. Placing the ABN in its own private extension.

This approach places the ABN in its own private extension. The inclusion of a private extension containing the ABN of the certificate subject is mandatory for an ABN-DSC type of certificate, however that extension is to be marked non-critical to maximise the interoperability with applications that are not aware of the ABN or the ABN-DSC.

3. OID for the ABN Extension

An Object Identifier, which indicates that the value in this extension is an ABN, has been registered by NOIE with Standards Australia. The registered OID is: 1.2.36.1.333.1 where the components represent:

1 =	ISO.
2 =	Member Body.
36 =	Australia.
1 =	NOIE.
333 =	Within the NOIE arc, this component represents Gatekeeper.
1 =	Subject Australian Business Number (ABN)

4. Extension structure

Figure 1 defines the ASN.1 structure of the ABN private extension for an ABN-DSC. The subject's ABN is identified by the OID shown in Figure 1. The extension value would contain the subject's ABN as an IA5String data type. Figure 2 provides an illustration of the extension structure.

```
id-pe-au-noie-subjectABN OBJECT IDENTIFIER ::= {
    iso (1) iso-member-body(2) australia (36) noie (001) gatekeeper (333) abn
    (1) }
ABNInfo ::= IA5String
```

Figure 1 - ASN.1 syntax for ABN Private Extension

Private Extension for ABN	
Field	Description / Example value
Certificate Extension identifier - OID	This OID identifies that this extension is defined by Australia NOIE, Gatekeeper for the purpose of containing the certificate subject's ABN
ABNInfo – IA5String	This field contains the value of the certificate subject's ABN.

Figure 2 - Extension structure for ABN-DSC

This approach has advantages in that it:

- follows the standard ASN.1 structure;
- provides a relatively simple specification for the extension; this is the simplest possible structure for the extension;
- is unambiguous for the ABN itself.

5. Sample ABN-DSC Authentication Certificate

The ABN-DSC requires two certificates and key pairs, authentication (or digital certificate) and confidentiality (or data encipherment). The following is a sample ABN-DSC authentication certificate including the ABN extension. The example does not necessarily illustrate typical values within the certificate, but rather is intended to illustrate the structure of the private extension containing the certificate subject's ABN.

For example, the sample end-entity certificate is issued by a certification authority with a fictitious distinguished name "cn=Generic Australia Pty Ltd ABN-DSC OCA, ou=Generic Australia Pty Ltd PKI Division, o=Generic Australia Pty Ltd, c=AU". The certificate subject's distinguished name is "cn=John Orville Smith, ou=Finance Department, o=Organisation Name, c=AU". The certificate contains a DSA public key, and is signed with DSA and SHA1.

Specifically, the example certificate contains the following information:

- The serial number is 34233.
- The certificate is signed with DSA and the SHA-1 hash algorithm.
- The issuer’s distinguished name is “cn=Generic Australia Pty Ltd ABN-DSC OCA, ou=Generic Australia Pty Ltd PKI Division, o=Generic Australia Pty Ltd, c=AU”.
- The subject’s distinguished name is “cn=John Orville Smith, ou= Finance Department, o=Organisation Name, c=AU”.
- The certificate is valid not before 15th August 2001 and not after 15th August 2002.
- The certificate contains a 1024 bit DSA public key with parameters.
- The certificate contains both authority and subject key identifier extensions generated in conformance with Gatekeeper X.509 Certificate and CRL Profile.
- The certificate contains a basic constraints extension that indicates it is not a CA certificate.
- The certificate contains a key usage extension that indicates it can only be used for a digital signature.
- The certificate contains a certificate policies extension that indicates the certificate is issued under certificate policies identified by OID “1.2.36.1.123.2” and “1.2.36.123.4”.
- The certificate contains a private extension which contains the ABN, in accordance with the selected approach.

The following is an annotated hex dump of a 945 byte version 3 certificate. The ABN private extension is identified by the OID "1.2.36.1.333.1".

```

0 30 941: SEQUENCE {
4 30 875:   SEQUENCE {
8 A0   3:     [0] {
10 02  1:      INTEGER 2
      :      }
13 02  3:      INTEGER 34233
18 30 11:      SEQUENCE {
20 06  7:      OBJECT IDENTIFIER dsaWithSha1 (1 2 840 10040 4 3)
29 05  0:      NULL
      :      }
31 30 146:     SEQUENCE {
34 31 11:      SET {
36 30  9:      SEQUENCE {
38 06  3:      OBJECT IDENTIFIER countryName (2 5 4 6)
43 13  2:      PrintableString 'AU'
      :      }
47 31 34:      SET {
49 30 32:      SEQUENCE {
51 06  3:      OBJECT IDENTIFIER organizationName (2 5 4 10)
56 13 25:      PrintableString 'Generic Australia Pty Ltd'
      :      }
83 31 47:      SET {
85 30 45:      SEQUENCE {
87 06  3:      OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
92 13 38:      PrintableString 'Generic Australia Pty Ltd PKI Division'
      :      }

```

```

:
:
132 31 46: SET {
134 30 44: SEQUENCE {
136 06 3: OBJECT IDENTIFIER commonName (2 5 4 3)
141 13 37: PrintableString 'Generic Australia Pty Ltd ABN-DSC OCA'
:
:
:
:
180 30 30: SEQUENCE {
182 17 13: UTCTime '010814232333Z'
197 17 13: UTCTime '020814232333Z'
:
:
212 30 99: SEQUENCE {
214 31 11: SET {
216 30 9: SEQUENCE {
218 06 3: OBJECT IDENTIFIER countryName (2 5 4 6)
223 13 2: PrintableString 'AU'
:
:
:
227 31 26: SET {
229 30 24: SEQUENCE {
231 06 3: OBJECT IDENTIFIER organizationName (2 5 4 10)
236 13 17: PrintableString 'Organisation Name'
:
:
:
255 31 27: SET {
257 30 25: SEQUENCE {
259 06 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
264 13 18: PrintableString 'Finance Department'
:
:
:
284 31 27: SET {
286 30 25: SEQUENCE {
288 06 3: OBJECT IDENTIFIER commonName (2 5 4 3)
293 13 18: PrintableString 'John Orville Smith'
:
:
:
}
}
}
313 30 439: SEQUENCE {
317 30 299: SEQUENCE {
321 06 7: OBJECT IDENTIFIER dsa (1 2 840 10040 4 1)
330 30 286: SEQUENCE {
334 02 129: INTEGER
:
: 00 D7 25 F1 ED 0B 13 14 D6 4C 0D AD 20 A4 DF F7
: 03 A8 A3 2E 3E 34 77 F3 4F 4F 2A 4F 29 91 88 8C
: E5 AC 01 37 BA 92 3B 5E 3C A5 3C 86 8B 66 D6 A2
: 1F 7E 53 90 35 10 AD 15 BC 1B E6 E0 A1 71 E5 D0
: A6 14 6D 82 5E E3 63 AC 9E 03 15 C5 B9 BF B3 5E
: A8 DC DE D2 5B C9 67 D2 33 14 C9 F8 21 96 CD FE
: CA A3 3F 1B EF E0 13 3D C1 ED AB 3B B8 FC 0A E0
: 6F B2 79 AF C6 12 94 97 22 17 4C BC C7 B6 82 1D
: [ Another 1 bytes skipped ]
466 02 21: INTEGER
: 00 EE 80 E0 19 73 B5 03 DF BD 2E 9E 96 BC A1 F3
: CB 62 8D 39 9B
489 02 128: INTEGER
: 50 7D 2E E1 97 62 56 13 9D 81 F3 22 C4 A8 2F 6F
: 85 9E 3A 7A 45 02 27 43 96 F4 2E 32 B7 14 EA 27
: 2A 4C DA 4D 52 EF 2F 40 19 05 AA 5B 7D 78 5D 0D
: A8 08 5C E9 88 EC DB 9E B3 5C D4 40 AB 01 D1 B1
: 69 8B 26 F3 B2 61 A2 FF 12 C6 CF 85 80 5F 32 94
: 63 5D 00 85 79 F1 05 28 80 0A 24 3E CF 8E 80 13
: E3 20 9A EF 82 A6 0D A3 2C 02 41 AA 15 65 46 B5
: B0 21 3C 45 75 75 1D 41 86 4F D7 84 69 18 9D FA
:
:
:
}
}
}
620 03 133: BIT STRING 0 unused bits, encapsulates {
624 02 129: INTEGER
: 00 C8 BF 09 08 09 40 38 ED 31 80 33 7D B6 B3 DD
: 59 4B A7 37 CF 52 37 ED FF CD D0 35 D7 DB 26 59
: C6 E1 E7 23 4C 32 4D B5 06 41 A3 0C 73 BE 4F B4

```

```

:          EC 56 F1 BA 80 3A 0C 47 DD 66 8E 72 A9 93 E6 5F
:          76 04 30 FD 25 7F DB 4A D9 04 A4 7F 5D A2 6A 43
:          6C 7D 1A 22 7F 49 B9 45 48 0F B0 BD 73 25 88 2D
:          A4 84 DE 07 B5 0C B9 97 F0 32 93 E6 35 5D 6A 26
:          6E 08 AA 7F 20 83 15 BC 06 95 99 81 BE 0F 13 9D
:          [ Another 1 bytes skipped ]
:          }
:          }
756 A3 125: [3] {
758 30 123: SEQUENCE {
760 30 17: SEQUENCE {
762 06 3: OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
767 04 10: OCTET STRING, encapsulates {
769 04 8: OCTET STRING
:          49 56 D2 49 96 74 31 23
:          }
:          }
779 30 19: SEQUENCE {
781 06 3: OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
786 04 12: OCTET STRING, encapsulates {
788 30 10: SEQUENCE {
790 80 8: [0]
:          40 32 BE DF E0 54 ED 65
:          }
:          }
800 30 25: SEQUENCE {
802 06 3: OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
807 04 18: OCTET STRING, encapsulates {
809 30 16: SEQUENCE {
811 30 6: SEQUENCE {
813 06 4: OBJECT IDENTIFIER '1 2 36 123 2'
:          }
819 30 6: SEQUENCE {
821 06 4: OBJECT IDENTIFIER '1 2 36 123 4'
:          }
:          }
:          }
827 30 12: SEQUENCE {
829 06 3: OBJECT IDENTIFIER basicConstraints (2 5 29 19)
834 01 1: BOOLEAN TRUE
837 04 2: OCTET STRING, encapsulates {
839 30 0: SEQUENCE {}
:          }
841 30 15: SEQUENCE {
843 06 3: OBJECT IDENTIFIER keyUsage (2 5 29 15)
848 01 1: BOOLEAN TRUE
851 04 5: OCTET STRING, encapsulates {
853 03 3: BIT STRING 0 unused bits
:          '0000000000000001'B (bit 0)
:          }
858 30 23: SEQUENCE {
860 06 6: OBJECT IDENTIFIER '1 2 36 1 333 1'
868 04 13: OCTET STRING, encapsulates {
870 16 11: IA5String '12345678912'
:          }
:          }
:          }
883 30 11: SEQUENCE {
885 06 7: OBJECT IDENTIFIER dsaWithShal (1 2 840 10040 4 3)
894 05 0: NULL
:          }
896 03 47: BIT STRING 0 unused bits, encapsulates {
899 30 44: SEQUENCE {
901 02 20: INTEGER
:          27 63 23 22 E6 FF 65 79 6E 79 DB 02 A5 32 3E F7

```

```
          :          7E 93 98 FC
923 02   20:        INTEGER
          :          39 B2 3C 4E 86 2D 65 C5 46 5A F3 B1 E2 96 4D 64
          :          DD 15 F2 31
          :          }
          :        }
          :      }
```

Annex A - ASN.1 Module using 1988 Syntax

```
NOIEgatekeeperABNDSExt DEFINITIONS EXPLICIT TAGS ::=
    BEGIN
        -- EXPORTS ALL --
        -- NOIE Gatekeeper defined Object Identifiers
        -- Certificate's subject ABN identifier
        id-pe-au-ato-subjectABN OBJECT IDENTIFIER ::= {
            iso (1) iso-member-body(2) australia (36) noie (1) gatekeeper(333)
            abn (1) }
        -- Subject ABN
        ABNInfo ::= IA5String
    END
```