1. Defect Report Number:
Title: Authority Key Identifier Format

2. Source: Santosh Chokhani, US

3. Addressed to:

4. (a)
(b)

5. Date circulated to WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning:
ITU-T X.509 (1997) | ISO/IEC 9594-8:1997

8. Qualifier:

Error

9. References in Document:

Clause 12.2.2.1 (error)

10. Nature of Defect:

The authority key identifier and subject key identifier extensions are defined primarily for the purpose of oath discovery. The authority key identifier extension permit two syntaxes. One syntax is the 2-tuple authorityCertIssuer, authorityCertSerialNumber.

The authority key identifier extension with this syntax has two problems: one due the difference in syntax with the subject key identifier, it can not be used for matching rule during path development; two, use of this extension to get a certificate can lead to not discovering legitimate paths when the CA is certified by more than one CA.

It seems that the only purpose the 2-tuple for of extension can serve is to provide a hint to the client about a preferred certification path.

Given, that the following alternatives are suggested.

11. Solution recommended by the Source:

The first alternative is to deprecate the 2-tuple for of the extension. In that case, section 12.2.2.1 will become:

12.2.2.1 Authority key identifier field

This field, which may be used as either a certificate extension or CRL extension, identifies the public key to be used to verify the signature on this certificate or CRL. It enables distinct keys used by the same CA to be distinguished (e.g. as key updating occurs). This field is defined as follows:

```
authorityKeyIdentifier EXTENSION ::= {
        SYNTAX                  AuthorityKeyIdentifier
        IDENTIFIED BY       id-ce-authorityKeyIdentifier }

AuthorityKeyIdentifier ::= SEQUENCE {
        keyIdentifier                      [0] KeyIdentifier}


KeyIdentifier ::= OCTET STRING
```

This extension is always non-critical.

Another alternative is to require that when the extension is present, the key identifier form shall at least be present. Furthermore, the instruction can state that the key identifier form shall be used path discovery and the issuer, serial number form shall be used only for giving preference to a certificate. Section 12.2.2.1 will change as follows:

12.2.2.1 Authority key identifier field

This field, which may be used as either a certificate extension or CRL extension, identifies the public key to be used to verify the signature on this certificate or CRL. It enables distinct keys used by the same CA to be distinguished (e.g. as key updating occurs). This field is defined as follows:

```
authorityKeyIdentifier EXTENSION ::= {
        SYNTAX                  AuthorityKeyIdentifier
        IDENTIFIED BY       id-ce-authorityKeyIdentifier }

AuthorityKeyIdentifier ::= SEQUENCE {
        keyIdentifier                      [0] KeyIdentifier

        authorityCertIssuer                     [1] GeneralNames              OPTIONAL,
        authorityCertSerialNumber [2] CertificateSerialNumber  OPTIONAL }
        ( WITH COMPONENTS        {..., authorityCertIssuer PRESENT,
                                authorityCertSerialNumber PRESENT} |
         WITH COMPONENTS         {..., authorityCertIssuer ABSENT,
                                authorityCertSerialNumber ABSENT} )

KeyIdentifier ::= OCTET STRING
```

The key may be identified by an explicit key identifier in the **keyIdentifier** component, or by both explicit key identifier and identification of a certificate for

the key. If both forms of identification are used then the certificate or CRL issuer shall ensure they are consistent. A key identifier shall be unique with respect to all key identifiers for the issuing authority for the certificate or CRL containing the extension. An implementation which supports this extension is not required to be able to process all name forms in the **authorityCertIssuer** component. (See 12.3.2.1 for details of the **GeneralNames** type.)
Certification authorities shall assign certificate serial numbers such that every (issuer, certificate serial number) pair uniquely identifies a single certificate.
The key identifier form can be used to select a CA certificate during path discovery. The authorityCertIssuer, authoritySerialNumber tuple can be used only to provide preference to one certificate over others during path discovery.

This extension is always non-critical.

Finally, the third alternative is to just provide guidance without requiring the presence of the key identifier form.

12.2.2.1 Authority key identifier field

This field, which may be used as either a certificate extension or CRL extension, identifies the public key to be used to verify the signature on this certificate or CRL. It enables distinct keys used by the same CA to be distinguished (e.g. as key updating occurs). This field is defined as follows:

```
authorityKeyIdentifier EXTENSION ::= {
        SYNTAX              AuthorityKeyIdentifier
        IDENTIFIED BY       id-ce-authorityKeyIdentifier }

AuthorityKeyIdentifier ::= SEQUENCE {
        keyIdentifier               [0] KeyIdentifier              OPTIONAL,

        authorityCertIssuer                  [1] GeneralNames         OPTIONAL,
        authorityCertSerialNumber [2] CertificateSerialNumber  OPTIONAL }
        ( WITH COMPONENTS        {..., authorityCertIssuer PRESENT,
                            authorityCertSerialNumber PRESENT} |
         WITH COMPONENTS         {..., authorityCertIssuer ABSENT,
                            authorityCertSerialNumber ABSENT} )

KeyIdentifier ::= OCTET STRING
```

The key may be identified by an explicit key identifier in the **keyIdentifier** component, identification of a certificate (using issue and issuer serial number) or by both explicit key identifier and identification of a certificate for the key. If both forms of identification are used then the certificate or CRL issuer shall ensure they are consistent. A key identifier shall be unique with respect to all key identifiers for the issuing authority for the certificate or CRL containing the extension. An implementation which supports this extension is not required to be able to process all name forms in the **authorityCertIssuer** component. (See 12.3.2.1 for details of the **GeneralNames** type.)

Certification authorities shall assign certificate serial numbers such that every (issuer, certificate serial number) pair uniquely identifies a single certificate. The key identifier form can be used to select CA certificates during path discovery. The authorityCertIssuer, authoritySerialNumber tuple can only be used to provide preference to one certificate over others during path discovery.

This extension is always non-critical.