pkix

package | standard library

Version: go1.20.1 Latest | Published: Feb 14, 2023 | License: BSD-3-Clause | Imports: 5 | Imported by: 13,124

Details Valid go.mod file | Redistributable license | Tagged version | Stable version

Learn more

Repository cs.opensource.google/go/go

Links Report a Vulnerability

Documentation

Documentation

Overview

Package pkix contains shared, low level structures used for ASN.1 parsing and serialization of X.509 certificates, CRL and OCSP.

Index

type AlgorithmIdentifier
type AttributeTypeAndValue
type AttributeTypeAndValueSET
type CertificateList DEPRECATED
    func (certList *CertificateList) HasExpired(now time.Time) bool
type Extension
type Name
    func (n *Name) FillFromRDNSequence(rdns *RDNSequence)
    func (n Name) String() string
    func (n Name) ToRDNSequence() (ret RDNSequence)
type RDNSequence
    func (r RDNSequence) String() string
type RelativeDistinguishedNameSET
type RevokedCertificate
type TBSCertificateList DEPRECATED

Constants

This section is empty.

Variables

This section is empty.

Functions

This section is empty.

Types

type AlgorithmIdentifier

```
type AlgorithmIdentifier struct {
    Algorithm  asn1.ObjectIdentifier
    Parameters asn1.RawValue `asn1:"optional"`
}
```

AlgorithmIdentifier represents the ASN.1 structure of the same name. See RFC 5280, section 4.1.1.2.

type AttributeTypeAndValue

```
type AttributeTypeAndValue struct {
    Type  asn1.ObjectIdentifier
    Value any
}
```

AttributeTypeAndValue mirrors the ASN.1 structure of the same name in RFC 5280, Section 4.1.2.4.

type AttributeTypeAndValueSET

added in go1.3

```
type AttributeTypeAndValueSET struct {
    Type  asn1.ObjectIdentifier
    Value [][]AttributeTypeAndValue `asn1:"set"`
}
```

AttributeTypeAndValueSET represents a set of ASN.1 sequences of AttributeTypeAndValue sequences from RFC 2986 (PKCS #10).

type CertificateList DEPRECATED Show

type Extension

```
type Extension struct {
    Id       asn1.ObjectIdentifier
    Critical bool `asn1:"optional"`
```

```
    Value    []byte
}
```

Extension represents the ASN.1 structure of the same name. See RFC 5280, section 4.2.

type Name

```
type Name struct {
    Country, Organization, OrganizationalUnit []string
    Locality, Province                        []string
    StreetAddress, PostalCode                 []string
    SerialNumber, CommonName                  string

    // Names contains all parsed attributes. When parsing distinguished names,
    // this can be used to extract non-standard attributes that are not parsed
    // by this package. When marshaling to RDNSequences, the Names field is
    // ignored, see ExtraNames.
    Names []AttributeTypeAndValue

    // ExtraNames contains attributes to be copied, raw, into any marshaled
    // distinguished names. Values override any attributes with the same OID.
    // The ExtraNames field is not populated when parsing, see Names.
    ExtraNames []AttributeTypeAndValue
}
```

Name represents an X.509 distinguished name. This only includes the common elements of a DN. Note that Name is only an approximation of the X.509 structure. If an accurate representation is needed, asn1.Unmarshal the raw subject or issuer as an RDNSequence.

func (*Name) FillFromRDNSequence

```
func (n *Name) FillFromRDNSequence(rdns *RDNSequence)
```

FillFromRDNSequence populates n from the provided RDNSequence. Multi-entry RDNs are flattened, all entries are added to the relevant n fields, and the grouping is not preserved.

func (Name) String

added in go1.10

```
func (n Name) String() string
```

String returns the string form of n, roughly following the RFC 2253 Distinguished Names syntax.

func (Name) ToRDNSequence

```
func (n Name) ToRDNSequence() (ret RDNSequence)
```

ToRDNSequence converts n into a single RDNSequence. The following attributes are encoded as multi-value RDNs:

- Country

- Organization
- OrganizationalUnit
- Locality
- Province
- StreetAddress
- PostalCode

Each ExtraNames entry is encoded as an individual RDN.

type RDNSequence

```
type RDNSequence []RelativeDistinguishedNameSET
```

func (RDNSequence) String

added in go1.10

```
func (r RDNSequence) String() string
```

String returns a string representation of the sequence r, roughly following the RFC 2253 Distinguished Names syntax.

type RelativeDistinguishedNameSET

```
type RelativeDistinguishedNameSET []AttributeTypeAndValue
```

type RevokedCertificate

```
type RevokedCertificate struct {
    SerialNumber   *big.Int
    RevocationTime time.Time
    Extensions     []Extension `asn1:"optional"`
}
```

RevokedCertificate represents the ASN.1 structure of the same name. See RFC 5280, section 5.1.

type TBSCertificateList DEPRECATED Show

Source Files

View all

pkix.go