# PKI profile for IPsec VPNs

Paul Hoffman, Director
VPN Consortium

# What is covered in this proposal

- Much of what was in the 1990 proposal, but brought up to date with more years of experience
- Identities: Name and SubjectAltName fields
- Key usage field
- Certificate expiration during an SA
- Required algorithms
- CERT and CERTREQ payloads
- Path validation
- Certificate revocation
- Enrollment for devices

# Basic assumptions

- The purpose of the certificate is to identify a device (a gateway or a remote access computer) to a relying gateway
- Both parties trust the CA fully
- In the great majority of cases, the parties will be (or at least control) their own CA
- PKIX is full of features that are not needed for IPsec

# Identities: Name and SubjectAltName

- The main use of identities from certificates in IPsec is to match access rights with requested proposals
- There is no need to match the IP address of the supplying party with the identity in the cert
- PKIX naming is a mess
- Certs should have null Subject, and use a small number of SubjectAltName types

# Key usage field

- Useful for generic CAs who are issuing certificates for a variety of purposes, not useful for CAs aimed at IPsec
- Relying party should ignore the key usage

# Certificate expiration during an SA

- CAs pick certificate expiration for many reasons, some of them silly
- Some VPN IPsec environments purposely create short-lived certs to limit access
- IPsec devices should note the expiration date on the cert and not create an SA that lasts beyond it
- Side effect: IPsec devices need reliable clocks

# Required algorithms

- This is covered in RFC 3279
- Must be able to handle a cert with sha-1WithRSAEncryption over an rsaEncryption key

# CERT and CERTREQ payloads

- Still wide confusion and debate over when the payloads should/must appear, and what they mean
- This has caused most of the lack of interoperability in IKEv1 using certificates
- Maybe should be a separate profile

# Path validation

- Devices must either be able to do full and correct path validation, or must fail when they get a chain
- Most environments are fine without paths
- Trust anchors do not need to be root certificates

# Certificate revocation

- This is still a mess in the PKI world
- Devices must be able to process and cache CRLs they get during IKE
- This should be covered in the other pki4ipsec documents

# Enrollment for devices

- PKCS10 copy-and-paste is near-universal
- We should profile it (ASCII armor words, use of CRLFs, etc.)
- SCEP is widely-used but not that interoperable
- However, real (that is, scalable) enrollment should be covered in the other pki4ipsec documents

# Summary

- Make this usable in a simple fashion without reducing actual security
- Be willing to break some current implementations, but make it easy to fix them
- Acknowledge that we have done an inadequate job of specifying this before, and fix it