Traditional Approach
Plat du jour
+
A-la-carte
MUST implement

Becomes obsolete
A-la-carte

Combinatorial explosion
Hidden Constraints

Box says ‘supports SHA-1, SHA-256, RSA, DSA’

BUT

DSA implementation does not support SHA-256
Result

Many variations to test
Many configurations for security analysis
Real ‘must implement’ deviates from specification
Hidden constraints are not exposed
Objectives

Constrain number of variations
Allow for specialty (vanity) crypto
Proposal

Quantum Profiles
Each Profile defines

One encryption, one digest, one MAC, one key exchange, one signature, &ct.

Has unique URI

[Parameters, Modes]
Finite Field Profile

RSA
SHA2
HMAC-SHA2
AES
One C18N
ECC Profile

NIST Suite B
One C18N
SHA3 Profile

To be released 2009/2010
Non-Standard Profile

NIST Suite A
Private definition
Parameters / Modes

Limited, discrete options

Master profile specifies set of sub profiles
Finite Field Profile

Level1: RSA2048, SHA256, AES128
Level1a: RSA4096, SHA256, AES128
Level2: RSA3072, SHA386, AES192
Level3: RSA4096, SHA512, AES256
Level3x = Level1 + Level1a + Level2 + Level3
Finite Field Profile v2007

Level1: RSA2048, SHA256, AES128
Level2: RSA4096, SHA256, AES128
Level3: RSA4096, SHA512, AES256

Level3x = Level1 + Level2 + Level3
Finite Field Profile v2009

Level1: RSA2048-RND-PSS, SHA256, AES128
Level2: RSA4096-RND-PSS, SHA256, AES128
Level3: RSA4096-RND-PSS, SHA512, AES256
URIs

e.g. http://w3.org/2008/xmlsec/profile-ff-level1

[Intentionally opaque]
Question

Specify Crypto and XML issues in same profile
Specify separate profiles for crypto and XML