Algorithm Profiles

Phillip Hallam-Baker

Principal Scientist

VeriSign Inc.

Traditional Approach

VeriSign

Plat du jour

+

A-la-carte

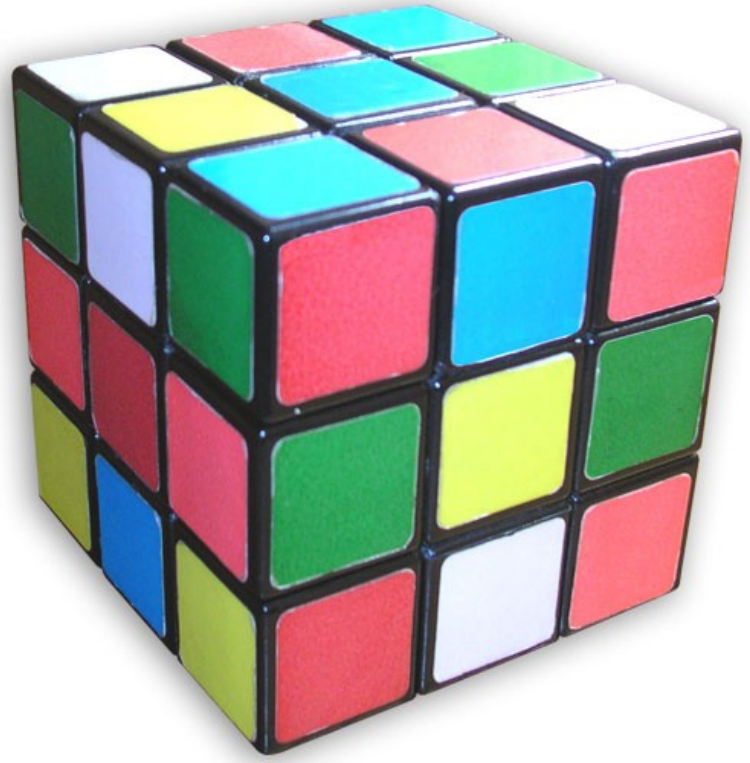
VeriSign

MUST implement

Becomes obsolete

VeriSign

A-la-carte



Combinatorial explosion

VeriSign

Hidden Constraints

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

BUT

DSA implementation does not support SHA-256

VeriSign

Result

Many variations to test

Many configurations for security analysis

Real ‘must implement’ deviates from specification

Hidden constraints are not exposed

VeriSign

Objectives

Constrain number of variations

Allow for specialty (vanity) crypto

VeriSign

Proposal

Quantum Profiles

VeriSign

Each Profile defines

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

Has unique URI

[Parameters, Modes]

VeriSign

Finite Field Profile

RSA
SHA2
HMAC-SHA2
AES
One C18N

VeriSign

ECC Profile

NIST Suite B

One C18N

VeriSign

SHA3 Profile

To be released 2009/2010

VeriSign

Non-Standard Profile

NIST Suite A

Private definition

VeriSign

Parameters / Modes

Limited, discrete options

Master profile specifies set of sub profiles

VeriSign

Finite Field Profile

Level1: RSA2048, SHA256, AES128

Level1a: RSA4096, SHA256, AES128

Level2: RSA3072, SHA386, AES192

Level3: RSA4096, SHA512, AES256

Level3x = Level1 + Level1a + Level2 + Level3

VeriSign

Finite Field Profile v2007

Level1: RSA2048, SHA256, AES128

Level2: RSA4096, SHA256, AES128

Level3: RSA4096, SHA512, AES256

Level3x = Level1 + Level2 + Level3

VeriSign

Finite Field Profile v2009

Level1: RSA2048-RND-PSS, SHA256, AES128

Level2: RSA4096-RND-PSS, SHA256, AES128

Level3: RSA4096-RND-PSS, SHA512, AES256

VeriSign

URIs

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

[Intentionally opaque]

VeriSign

Question

Specify Crypto and XML issues in same profile

Specify separate profiles for crypto and XML

VeriSign