Beyond FIPS

Baseline Requirements

“The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.”

- at least FIPS 140 level 3
- an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats

FIPS?

- FIPS = Federal Information Processing Standards
- Issued by the National Institute of Standards and Technology, a part of the Department of Commerce, part of the United States federal Government
- Focused on setting standards for government agencies

FIPS 140

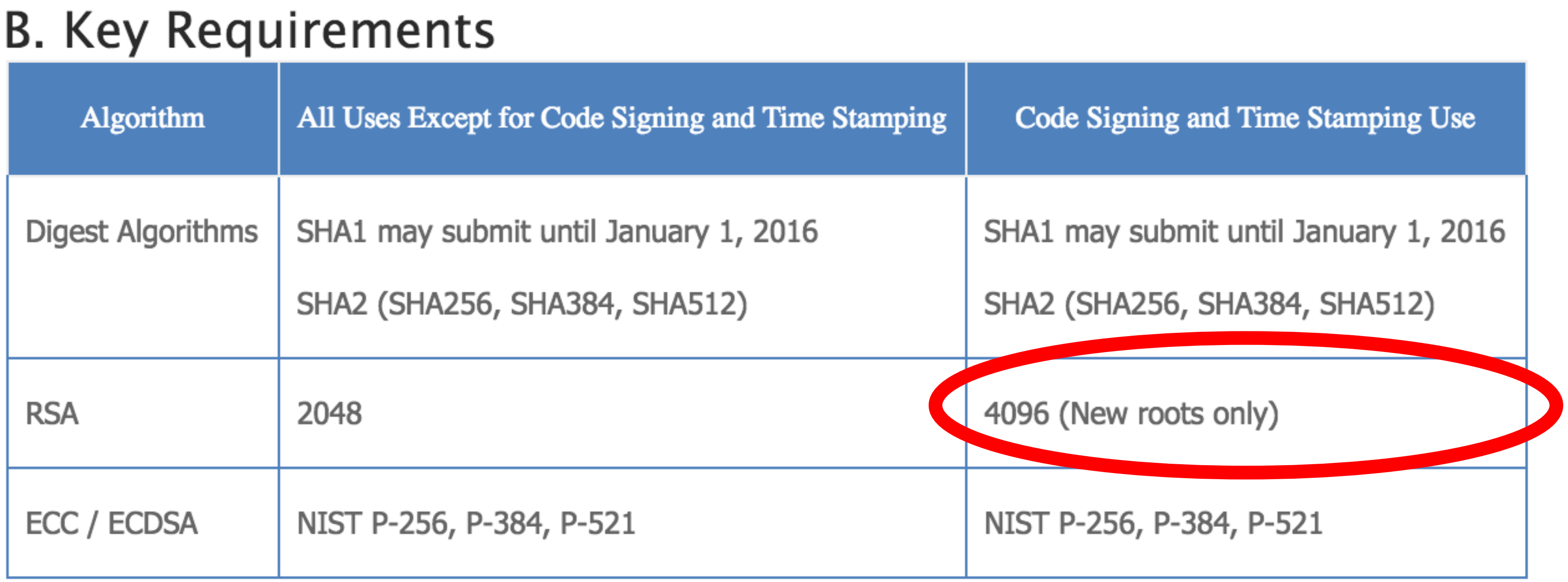
- “Security Requirements for Cryptographic Modules”
- References a number of other FIPS and NIST “Special Publications”
- Certification program run by NIST and the Communications Security Establishment (part of the Department of National Defence, part of the Government of Canada)

- All certified modules must have “FIPS mode”
- May have a non-FIPS mode

FIPS Mode

- Only enable algorithms and parameters specified FIPS and NIST SPs
- Public Key algorithms:
  - RSA with 512, 768, 1024, and 1536 bit long p & q (i.e. 1024, 1536, 2048, and 3072 bit long n)
  - DSA with similar L sizes
  - ECDSA over NIST defined curves (including P-256, P-384, and P-521)
- Hash Algorithms:
  - MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, and SHA3 family

Microsoft Requirements



B. Key Requirements

Algorithm	All Uses Except for Code Signing and Time Stamping	Code Signing and Time Stamping Use
Digest Algorithms	SHA1 may submit until January 1, 2016 SHA2 (SHA256, SHA384, SHA512)	SHA1 may submit until January 1, 2016 SHA2 (SHA256, SHA384, SHA512)
RSA	2048	4096 (New roots only)
ECC / ECDSA	NIST P-256, P-384, P-521	NIST P-256, P-384, P-521

IETF/IRTF Drafts

- CFRG and CURDLE WG
- EdDSA in two modes, “combined” and prehash
- Two curves specified: 25519 and 448-Goldilocks
- Same curves already in published RFC for key exchange

- Deterministic ECDSA

Other National Standards

- SM2 and SM3: China Office of State Commercial Cryptography Administration
- GOST R 34.10-2012: Euroasian Interstate Council for Standardization, Metrology and Certification
- ECGDSA (Germany)
- ECKCDSA (Korea)

Post-Quantum

- Merkle Signature Scheme
- Ring-Learning with Errors (RLWE-SIG or GLP)
- Elliptic Curve Isogenies

Why FIPS?

- Key Pair generation and validation
  - Ensure that proper generation procedure is followed
  - Ensure that appropriate TRNG/CSPRNG/DRBG is used
  - Validate resulting private key components (e.g. are p and q really prime?)
- Signature creation
  - Some signature algorithms require random input

Options

- Non-FIPS mode
- Common Criteria: Does SSCD meet CA needs?
- Other standards?
- Only protect key using HSM, allow residing in memory?
- Programmable HSMs