



Příloha: Technické parametry související s implementací certifikátů SHA-2 v komerčně dostupných produktech společnosti Microsoft

Validace (ověření) certifikátů SHA-2 je podporováno v následujících produktech:

- Windows XP Service Pack 3
- Windows Vista
- Windows Server 2008 SP1
- Windows Server 2003 SP2 + speciální hotfix

Pod pojmem validace certifikátu rozumíme možnost ověřit podepsaný certifikát či řetězec certifikátů, které jsou například použity v rámci https relace.

Validace v žádném případě neznamená, že zcela všechny SHA-2 algoritmy jsou zároveň implementovány v rámci Secure-MIME (SMIME), nebo že mohou být využity aplikacemi, které používají Crypto-API (CAPI).

V rámci Windows XP SP3 je implementována podpora SHA-2 hashovacích algoritmů (SHA256, SHA384 a SHA512) pro validaci X.509 certifikátů. Implementace je provedena v rámci kryptografické knihovny rsaenh.dll.

Implementace SHA-2 algoritmů v rámci Windows XP SP3 slouží pouze k validaci certifikátu.

Považujeme za nutné zdůraznit fakt, že validace certifikátu není v žádném případě hashování, podepisování, kódování nebo dekódování binárních dat, v tomto případě za využití CAPI 2.0 (SHA-2 rodina, AES).

Komplexní implementace CAPI 2.0, umožňující plné použití algoritmů SHA-2, je součástí produktů:

- Windows Vista
- Windows Serveru 2008 SP1

Z tohoto důvodu je nutné pro plné aktivní používání (hashování, podepisování, kódování nebo dekódování binárních dat) SHA-2 pro SMIME provést upgrade operačního systému na prodávaný os Windows Vista nebo později na Windows 7.

Vytváření certifikátů s podporou těchto funkcí je podporováno na již volně dostupném serverovém operačním systému:

- Windows Server 2008 SP1 (Active Directory Certificate Services)

Stále velice často využívaný serverový operační systém Windows Server 2003 neobsahuje plnou implementaci CAPI2.0 a proto Certifikační autorita vybudována na této platformě algoritmy SHA-2 nepodporuje a podporovat nebude.