SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã,'MD5ç½²å••ã•‹ã,‰SHA-1ç½²å••ã•«

Category : ã,µãƒ¼ãƒ•ç®¡ç•†æ—¥è¨˜
Published by M-naka on 2009/1/11

JVNVU#836068

MD5ã,¢ãƒ«ã,´ãƒªã,ºãƒ ã•¸ã•®è¡•ç°•æ"»æ'ƒï¼ˆCollison Attackï¼‰ã•«ã,ˆã,Šã€•ç½²å••ã,¢ãƒ«ã,´ãƒªã,ºãƒ ã•«MD5ã,'ä½¿ç"¨ã•—ã•¦ã•„ã,‹SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã•®å•½é€ ã•«æˆ•åŠŸã•—ã•Ÿã€•ã•¨ã•®ã•"ã•¨ã€,æ¼"ç®—ã•«200å•°ã•®PS3ã,'ã,¯ãƒ©ã,¹ã,¿åŒ–ã•—ã•¦ä½¿ã•£ã•Ÿã••ã•†ã•ªã€,

ã•§ã€•verisign.co.jpã•«ã•¯æ˜Žè¨˜ã•¯ã•ªã•„ã,"ã• ã•'ã•©ã€•verisign.comã•«ã•¯ å•½é€ ã•§ã••ã•Ÿã•®ã•¯RapidSSLã•®SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã•¨æ˜Žè¨˜ã•Œã•,ã,‹ã€,

â€¦â€¦ã•£ã•¦ã€•ã,¦ãƒ•ã•§ä½¿ã•£ã•¦ã,‹ã•˜ã,ƒã,"ã€•RapidSSLã•®SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã€,

ç¢ºã•‹ã•«ãƒ–ãƒ©ã,¦ã,¶ã•‹ã,‰é›»å-•è¨¼æ˜Žæ›¸ã•®è©³ç´°ã,'è¦‹ã•¦ã•¿ã,‹ã•¨ã€•ç½²å••ã,¢ãƒ«ã,´ãƒªã,ºãƒ ã•¯MD5ã•«ã•ªã•£ã•¦ã,‹ã€,å½±éŸ¿ã•®ã•ªã•„EV SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã•¨ã•‹ã€•ã•Šé«˜ã,•ã•®æ³•ä°°å•'ã•'SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã•¯ã,„ã•¨ã,„ã•¨SHA-1ç½²å••ã• ã•£ã•Ÿã,‰ã•—ã••ã€,

ã,„ã•¨ã,„ã•¨MD5ã•«ã•¯æ½œåœ¨ç§„ã•«ã•,ã•£ã•Ÿè„†å¼±æ€§ã•§ã•¯ã•,ã,‹ã•—ã€•ã•¾ã•Ÿå•½é€ æˆ•åŠŸä°‹ä¾‹ã,'ã„ã•£ã•¦ç›´ã•¡ã•«MD5ç½²å••ã•®SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã•Œå…¨ã•¦ã,»ã,-ãƒ¥ã,¢ã•§ã•ªã•• ã•ªã,‹ã€•ã•¨ã•„ã•†ã,•ã•'ã•§ã•¯ã•ªã•„ã€,ã•Œã€•å®Ÿè¨¼ã••ã,Œã•Ÿã•®ã•¯ä°‹å®Ÿã•§ã•,ã,Šã€•ã••ã•®ã•¾ã•¾ã•«ã•—ã•¦ã•Šã••ã•®ã•¯ã•,ã•¾ã,Šå®œã•—ã•„è©±ã•§ã•¯ã•ªã•„ã€,

ã,¦ãƒ•ã•¯trusticoã•¨ã•„ã•†æµ·å¤–ã•®æ¥-è€…ã•‹ã,‰ã,ªãƒ³ãƒ©ã,¤ãƒ³ã•§RapidSSLã•®SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã,'å…¥æ‰‹ã•—ã•¦ã•„ã,‹ã•Œã€•ç™ºè¡Œæ‡ªä½"ã•¯GeoTrustã€•ã••ã•—ã•¦ã•©ã•"ã•®ä»²ä»‹æ¥-è€…ã,'é€šã•—ã•¦ã•„ã•¦ã,ã•"ã•®å••é¡Œã•¯å…±é€šã€,ã•§ã€•GeoTrustã€•ã•¨ã•„ã•†ã•‹GeoTrustã•®è¦ªä¼šç¤¾ã•®VeriSignã•¨ã•—ã•¦ã•¯ã€•ç½²å••ã,¢ãƒ«ã,´ãƒªã,ºãƒ ã,'SHA-1ã•«ã•—ã•ŸRapidSSLã•®SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã,'ç„¡å„Ÿã•§ç™ºè¡Œã•—ç›´ã•—ã•¦ã••ã,Œã,‹ã•¨ã•®ã•"ã•¨ã€,

https://www.geotrust.com/support/ssl-certificate-reissuance/

å†•ç™ºè¡Œã•«ã½"ã•Ÿã•£ã•¦ã•¯ä»¥ä¸‹ã•Œå¿…è¦•ã€,

â– ç™ºè¡Œæ¸ˆã•¿ã•®SSLã,µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã•®FQDN
â– ç™ºè¡Œæ™‚ã•«ä½¿ç"¨ã•—ã•Ÿç®¡ç•†è€…ãƒ¡ãƒ¼ãƒ«ã,¢ãƒ‰ãƒ¬ã,¹
â– CSR
ã€€â†'åˆ•å›žç™ºè¡Œæ™‚ã•¨ã•Œä¸€ã•§ã„è‰¯ã•„ã•Œã€•å†•ç"Ÿæˆ•ã•®æ–¹ã•Œæœ›ã•¾ã•—ã•„ã• ã,•ã•†ã€,

è¦•ã•¯FQDNã•§ç™ºè¡Œæ¸ˆãƒ»å†•ç™ºè¡Œå¯¾è±¡ã•‹ã,'èª¿ã•¹ã€•å¯¾è±¡ã•ªã,‰ã••ã•®ã•¾ã•¾ç„¡å„Ÿã•§æ‰‹ç¶šã••ã,'ã••ã•›ã•¦ã••ã,Œã,‹ã€•ã•¨ã•„ã•†ãƒ•ãƒ-ãƒ¼ã•«ã•ªã•£ã•¦ã•„ã,‹ã€,

ã€€ç”³ã•—è¾¼ã•¿
â†’ç”³ã•—è¾¼ã•¿æ‰¿èªç¢ºèªã•ãƒ¡ãƒ¼ãƒ«
â†’æ‰¿èªå¾Œã€•Webã•§CSRã‚’ã‚³ãƒ”ãƒšã•§å…¥åŠ›
â†’SSLã‚µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã•Œãƒ¡ãƒ¼ãƒ«ã•§å±Šã•„ã•¦ç‚µäº†

ã•“ã‚“ã•ªæ„Ÿã•˜ã€‚

ã•§ã€•Apacheã•¨ã•„ã•†ã•‹ã€•mod_sslã•«å†•ç™ºè¡Œã••ã‚Œã•ŸSSLã‚µãƒ¼ãƒ•è¨¼æ˜Žæ›¸ã‚’ç™»éŒ²ã€•Apacheã‚’å†•èµ·å‹•ã•—ã•¦ä½œæ¥-å®Œäº†ã€‚ãƒ–ãƒ©ã‚¦ã‚¶ã•¦ã•¶ã•§è¦‹ã‚‹ã•¨ç½²å••ã‚¢ãƒ«ã‚´ãƒªã‚ºãƒ ã•Œç¢ºã•‹ã•«SHA-1ã•«ã•ªã•£ã•¦ã•„ã‚‹ã€‚

ã•¡ã•ªã•¿ã•«æœŸé–“å†…å†•ç™ºè¡Œã•ªã•®ã•§ã€•æœ‰åŠ¹æœŸé™•ã•¯å¾“æ•¥é€šã‚Šã€‚ã•¾ã€•ç„¡å„Ÿå¯¾å¿œã• ã•—ã€•å½“ã•Ÿã‚Šå‰•ã•¨ã•„ã•^ã•°å½“ã•Ÿã‚Šå‰•ã•ªã•®ã• ã•Œã€‚