

VETUMA-PALVELUN PALVELINVARMENTEET

Sisällysluettelo

1. Johdanto	3
2. Testiympäristö.....	3
2.1 Testiympäristön palvelinvarmenne.....	3
2.2 Testiympäristön palvelinvarmenteen myöntäjä	4
3. Tuotantoympäristö.....	5
3.1 Palvelinvarmenne	5
3.2 Palvelinvarmenteen myöntäjä	5
3.3 Myöntäjävarmenteen juurivarmenne.....	6
4. Käyttäjähallinta.....	7
4.1 Palvelinvarmenne	7
4.2 Palvelinvarmenteen myöntäjä	8
4.3 Myöntäjävarmenteen juurivarmenne.....	8

1. JOHDANTO

Tämä dokumentti kuvaa VETUMA-palvelussa käytössä olevat palvelinvarmenteet. Dokumentti on Vetuma Rajapintakuvaus –dokumentin liite 1.

Dokumentissa on kuvattu varmenteista tärkeimpien kenttien arvot. Palvelussa käytetään kahden eri myöntäjän varmenteita

VeriSign ja Fujitsu TopSEL CA

2. TESTIYMPÄRISTÖ

VETUMA-palvelun testiympäristön osoite on: <https://testitunnistus.suomi.fi>

Käytössä on Fujitsun TopSEL CA-myöntäjän allekirjoittamaa varmennetta.

2.1 Testiympäristön palvelinvarmenne

Kenttä	Arvo
Serial number	01:4D
Signature algorithm	md5RSA
Issuer	CN = Fujitsu TopSEL CA OU = Fujitsu Services Oy O = Fujitsu Services Oy L = Helsinki S = Helsinki C = FI
Valid from	28.10.2008
Valid to	27.10.2013
Subject	CN = testitunnistus.suomi.fi OU = Fujitsu Services Oy O = Fujitsu Services Oy L = Helsinki S = Helsinki C = FI
Thumbprint algorithm	sha1
Thumbprint	6A:78:73:FB:66:76:8E:7F:58:9C:29:0D:23:72:0A:7D:FC:F2:0D:FE

2.2 Testiympäristön palvelinvarmenteen myöntäjä

Testiympäristössä käytettävä Fujitsun Topsis CA varmenne on ladattavissa testipalvelun info-sivulta: <https://testitunnistus.suomi.fi/info/>

Kenttä	Arvo
Serial number	00
Signature algorithm	md5RSA
Issuer	CN = Fujitsu Topsis CA OU = Fujitsu Services Oy O = Fujitsu Services Oy L = Helsinki S = Helsinki C = FI
Valid from	4.11.2003 18:29:08
Valid to	1.11.2013 18:29:08
Subject	CN = Fujitsu Topsis CA OU = Fujitsu Services Oy O = Fujitsu Services Oy L = Helsinki S = Helsinki C= FI
Thumbprint algorithm	sha1
Thumbprint	ac c3 e3 8b 2c 70 a9 1b 8d 46 17 6a f3 b7 0b b7 75 73 4f 8c

3.TUOTANTOYMPÄRISTÖ

VETUMA-palvelun tuotantoympäristön osoite on: <https://tunnistus.suomi.fi>

Tuotantopalvelun varmenne on VeriSign-myöntäjän varmentaja. Tämä varmentaja on yleisimmissä selaimissa valmiiksi asennettu luotetuksi myöntäjäksi.

3.1 Palvelinvarmenne

Kenttä	Arvo
Serial number	3C:89:C1:87:39:D3:30:72:39:4C:DD:EC:08:38:68:23
Signature algorithm	PKCS #1 SHA-1 RSA-salauksella
Issuer	CN = O = VeriSign Trust Network OU= VeriSign, Inc.
Valid from	29.5.2008 13.04
Valid to	29.5.2010 13.04
Subject	CN = tunnistus.suomi.fi O = Fujitsu Services Oy OU = Valtiovarainministeriö L = Helsinki ST = Finland C = FI
Thumbprint algorithm	PKCS #1 SHA-1 RSA-salauksella
Thumbprint	BB:40:B8:CC:F9:F7:3C:2F:7F:79:97:7C:0F:0B:67:FF:9C:BA:45:41

3.2 Palvelinvarmenteen myöntäjä

Kenttä	Arvo
Serial number	25 4b 8a 85 38 42 cc e3 58 f8 c5 dd ae 22 6e a4
Signature algorithm	PKCS #1 SHA-1 RSA-salauksella
Issuer	OU = Class 3 Public Primary Certification Authority O = VeriSign, Inc. C = US

Valid from	17. huhtikuuta 1997 2:00:00
Valid to	25. lokakuuta 2011 1:59:59
Subject	OU = www.verisign.com/CPS Incorpor.by Ref. LIABILITY LTD.(c)97 VeriSign OU = VeriSign International Server CA - Class 3 OU = VeriSign, Inc. O = VeriSign Trust Network
Thumbprint algorithm	PKCS #1 SHA-1 RSA-salauksella
Thumbprint	c2 f0 08 7d 01 e6 86 05 3a 4d 63 3e 7e 70 d4 ef 65 c2 cc 4f

3.3 Myöntäjävarmenteen juurivarmenne

Kenttä	Arvo
Serial number	70 ba e4 1d 10 d9 29 34 b6 38 ca 7b 03 cc ba bf
Signature algorithm	PKCS #1 SHA-1 RSA-salauksella
Issuer	OU = Class 3 Public Primary Certification Authority O = VeriSign, Inc. C = US
Valid from	29. tammikuuta 1996 2:00:00
Valid to	2. elokuuta 2028 1:59:59
Subject	OU = Class 3 Public Primary Certification Authority O = VeriSign, Inc. C = US
Thumbprint algorithm	PKCS #1 SHA-1 RSA-salauksella
Thumbprint	74 2c 31 92 e6 07 e4 24 eb 45 49 54 2b e1 bb c5 3e 61 74 e2

4. KÄYTTÄJÄHALLINTA

VETUMA-palvelun testi- ja tuotantoympäristön käyttäjähallinnan palvelinvarmenne on VeriSign-myöntäjän wildcard-varmenne *.topsel.fi

Tuotantopalvelun käyttäjähallinnan osoite: <https://vetuma.topsel.fi>

Testiympäristön käyttäjähallinnan osoite: <https://vetumatest.topsel.fi>

4.1 Palvelinvarmenne

Kenttä	Arvo
Serial number	1C:CF:B4:BF:3A:87:B8:66:5D:E2:C4:F9:20:99:E5:0A
Signature algorithm	PKCS #1 SHA-1 RSA-salauksella
Issuer	CN = VeriSign Class 3 Secure Server CA OU = Terms of use at https://www.verisign.com/rpa (c)05 OU = VeriSign Trust Network O = VeriSign, Inc. C = US
Valid from	12.6.2008 3.00
Valid to	14.6.2009 2.59
Subject	CN = *.topsel.fi OU = Terms of use at www.verisign.com/rpa (c)05 OU = Fujitsu Topsel O = Fujitsu Services Oy L = Helsinki ST = Uusimaa C = FI
Thumbprint algorithm	PKCS #1 SHA-1 RSA-salauksella
Thumbprint	25 ab ad 7d 02 75 d4 2d 69 a9 a9 6b 33 97 0d f8 f8 48 9a 56

4.2 Palvelinvarmenteen myöntäjä

Kenttä	Arvo
Serial number	75:33:7D:9A:B0:E1:23:3B:AE:2D:7D:E4:46:91:62:D4
Signature algorithm	PKCS #1 SHA-1 RSA-salauksella
Issuer	OU = Class 3 Public Primary Certification Authority O = VeriSign, Inc. C = US
Valid from	19.1.2005 2.00
Valid to	19.1.2015 1.59
Subject	CN = VeriSign Class 3 Secure Server CA OU = Terms of use at https://www.verisign.com/rpa (c)05 OU = VeriSign Trust Network O = VeriSign, Inc. C = US
Thumbprint algorithm	PKCS #1 SHA-1 RSA-salauksella
Thumbprint	c3 7e 08 46 5d 91 36 cf 67 dc d7 a7 af af b8 22 c3 8b 04 74 d3 b1 60 bc e6 fe b7 44 12 81 5b 31 73 14 63 56 c6 72 2e d1 1a 03 43 5c 38 0a 50 4a 4d cd da b6 19 a8 f4 99 0d af e3 f7 d8 f1 75 28 65 f6 6a fe 9b f4 bd 52 d9 3f cb da 16 cb a5 9e 2e 8e 66 52 78 3d 26 fa fe 94 36 88 4a 95 5e 2a 4c 19 ef 6e fa 82 3f 2d 03 ef d6 28 b3 37 18 cf 42 b2 34 21 64 47 d3 20 6b 3a 4c dc e6 03 90 0c

4.3 Myöntäjävarmenteen juurivarmenne

Katso kpl 3.3