DATEVe:secure MAIL V1.1

DATEV eG

ISIS-MTT-Assessment Report

Version 1.1
Date 08. July 2004

Hans-Joachim Knobloch, Fritz Bauspiess

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Secorvo herewith confirms, that for the product

DATEVe:secure MAIL V1.1

manufactured by

DATEV eG

in combination with

Microsoft Office Outlook 2003

an ISIS-MTT-compliance assessment has been completed between 29 June 2004 and 06 July 2004.

The product is ISIS-MTT-compliant with respect to the Component Conformance Statement ref. no Secorvo-00005 provided

We recommend to award the

ISIS-MTT-conformance label ("ISIS-MTT-Siegel")

for the

product class "E-Mail-Client"

Reference-Number: Secorvo-00005

ISIS-MTT-Specification-Version: 1.1

ISIS-MTT-Test-Specification-Version: 1.0.2

ISIS-MTT Compliance Criteria Version 1.1

ISIS-MTT-Testbed Version 1.1 Build 5 SP1 (with modifications)

Karlsruhe, 08 July 2004

Fritz Bauspiess

Content

Acronyms

CA	Certificate Authority
CCS	Component Conformance Statement
CRL	Certificate Revocation List
CUT	Component under test
EE	End Entity
FC	Functionality Class
MIME	Multipurpose Internet Mail Extension
MS	Microsoft
OID	Object Identifier
PC/SC	Personal Computer / SmartCard
S/MIME	Secure MIME
USB	Universal Serial Bus

1 Summarized Assessment Results

DATEVe:secure MAIL V1.1 in combination with Microsoft Office Outlook 2003 belongs to the product class “E-Mail-Client”. Functionality classes 5, 8, 11, 12, 14, 15, 16, 18, 29 and 30 are declared to be conformant to ISIS-MTT and were tested during the compliance assessment.

Additionally, functionality class 21 (LDAP client) was also declared to be conformant to ISIS-MTT. According to the current version 1.0.2 of the ISIS-MTT-Test-Specification no tests are provided for this functionality class. Thus no corresponding tests had to be applied.

Two test cases for functionality classes

- FC16 “Processing of S/MIME Messages with signed data” and
- FC18 “Processing of a Multipart/Signed S/MIME Message”

failed.

Microsoft Office Outlook 2003 crashes if it is presented a malformed signed S/MIME Message with an empty signed attributes set in test cases TCPSD-1.12 and TCPSD-3.11.

However

- albeit this failure is relevant with respect to the robustness of the CUT, it does not affect interoperability.

  ISIS-MTT does not permit the generation of such an empty signed attributes set.

  According to P3.T5.#1 and P3.T5.#2 of the ISIS-MTT specification in combination with P3.T5.[1], at least the attributes *content-type* and *message-digest* must be contained in the signed attributes set, if this set is contained in the *SignerInfo* field.

  Additionally the ASN.1 notation given in RFC 3369 and cited in ISIS-MTT 1.1, Part 3, page 25 explicitely states

  SignedAttributes ::= SET SIZE (**1**..MAX) OF Attribute

  which also prohibits the generation of an empty signed attributes set.

  Thus in an ISIS-MTT compliant environment, an e-mail client never should receive such a malformed S/MIME message containing the optional field *signedAttrs* but with an empty attributes set.

- there is no requirement in the ISIS-MTT specification, that an e-mail client has to be able to cope with such a malformed S/MIME message. Failing the test cases TCPSD-1.12 and TCPSD-3.11 thus does not reflect a missing compliance of the CUT with respect to the ISIS-MTT specification.

Moreover the reason for this failure is located in the underlying system, namely in some runtime library of the Microsoft Internet Explorer installed with the operating system. It is therefore out of reach of the manufacturer. This failure is already passed on to Microsoft and is currently handled under service request number SRZ040511000654.

All other tests were passed, some with warning.

Therefore the overall result of the assessment with respect to compliance to the ISIS-MTT specification has to be declared as “**passed**”.

These are the summarized results of the tests applied:

FC	Description	Result
5	Processing of public key certificates	passed with warning
8	Processing of CRLs	passed with warning
11	Generation of an S/MIME Message for Enveloped Data	passed
12	Generation of an S/MIME Message for Signed Data	passed
14	Generation of a Multipart/Signed S/MIME Message	passed
15	Processing of an S/MIME Message for Enveloped Data	passed with warning
16	Processing of S/MIME Messages with signed data	failed
18	Processing of a Multipart/Signed S/MIME Message	failed
29	Processing of a valid, 3-step certificate path	passed
30	Processing of an invalid certificate path	passed

The tests were based on the ISIS-MTT Specification Version 1.1, Part 1 “Certificate and CRL Profile”, Part 3 “Message Formats” and Part 5 “Certificate Path Validation”.

The tests were performed using the ISIS-MTT testbed implementing the version 1.0.2 of the ISIS-MTT specification. Therefore some test steps are marked as ‘failed’, however these issues are resolved by the changes made in version 1.1. Explanations are given with the individual test steps.

None of the modifications in version 1.1 compared to version 1.0.2 of the ISIS-MTT specification has a negative effect on any test steps marked as passed by the testbed.

2 Test Group PROC-CERT

2.1 Test Case TCPPKC-1

Date: Wed Jun 30 15:36:08 CEST 2004

Test step 1 (Certificate)	passed
Test step 2 (signatureAlgorithm)	passed with warning
Test step 3 (signature)	passed
Test step 4 (version)	passed
Test step 5 (serialNumber)	passed
Test step 6 (issuer)	passed with warning
Test step 7 (validity)	passed
Test step 8 (subject)	passed with warning
Test step 9 (subjectPublicKeyInfo)	passed
Test step 10 (issuerUniqueID)	passed
Test step 11 (subjectUniqueID)	passed
Test step 12 (extensions)	passed with warning

Test case passed with warning

Note:

The warning in test step 8 is due to the fact that for the ISIS-MTT mandatory distinguished name attributes nameAtBirth (1.3.36.8.3.14), countryOfResidence (1.3.6.1.5.5.7.9.5), countryOfCitizenship (1.3.6.1.5.5.7.9.4), gender (1.3.6.1.5.5.7.9.3), placeOfBirth (1.3.6.1.5.5.7.9.2) and pseudonym (2.5.4.65) as well as for several ISIS-MTT recommended attributes, Outlook resp. Windows does not present the readable attribute name but the OID value to the user.

For increased usability of the product in an ISIS-MTT environment, we recommend that DATEV adds a translation table from OID to attribute name to the user documentation of DATEVe:secure MAIL.

2.2 Test Case TCPCRL-1

Date: Wed Jun 30 16:04:04 CEST 2004

Test step 1 (CertificateList)	passed
Test step 2 (signatureAlgorithm)	passed with warning
Test step 3 (signatureValue)	passed
Test step 4 (issuer)	passed with warning

Test step 5 (thisUpdate)	passed
Test step 6 (nextUpdate)	passed
Test step 7 (revokedCertificates)	passed
Test step 7 a) (userCertificate)	passed
Test step 7 b) (revocationDate)	passed
Test step 7 c) (crlEntryExtensions)	passed with warning
Test step 8 (crlExtensions)	passed

Test case passed with warning

3 Test Group G-SM/ED

3.1 Test Case TCGSMED-1

Date: Mon Jul 5 10:32:35 CEST 2004

Test step 1 (Content-Type)	failed
Test step 2 (Content-Transfer-Encoding)	passed
Test step 3 (Content-Disposition)	passed
Test step 4 (MIME entity with enveloped-data)	passed

Test case passed

Note:

The failure in test step 1 is due to the fact that Microsoft Outlook when sending S/MIME messages uses the experimental content-subtype "x-pkcs7-mime" instead of "pkcs7-mime" as it was required by ISIS-MTT 1.0.2. In ISIS-MTT 1.1 this experimental content-subtype MAY be used as well. Thus test step 1 hat to be considered as “passed” with respect to version 1.1 of the ISIS-MTT specification.

3.2 Test Case CMS/TCGED-1

Date: Mon Jul 5 10:32:35 CEST 2004

Test step 0 (parse ASN.1)	passed
Test step 1 (ContentType)	passed
Test step 2 (Version)	passed
Test step 3 (OriginatorInfo)	passed
Test step 4 (RecipientInfos)	passed
Test step 5 (KeyTransRecipientInfo (ktri))	passed
Test step 6 (ktriVersion)	passed

Test step 7 (ktriRecipientIdentifier)	passed
Test step 8 (ktriKeyEncryptionAlgorithm)	passed
Test step 9 (ktriEncryptedKey)	passed
Test step 10 (EncryptedContentInfoContentType)	passed
Test step 11 (EncryptedContentInfoEncryptionAlgorithm)	passed
Test step 12 (EncryptedContentInfoEncryptedContent)	passed
Test step 13 (UnprotectedAttributes)	passed

Test case passed

4 Test Group G-SM/SD

4.1 Test Case TCGSMSD-1

Date: Mon Jul 5 10:51:02 CEST 2004

Test step 1 (Content-Type)	failed
Test step 2 (Content-Transfer-Encoding)	passed
Test step 3 (Content-Disposition)	passed
Test step 4 (MIME entity with enveloped-data)	failed

Test case passed

Notes:

The failure in test step 1 is due to the fact that Microsoft Outlook when sending S/MIME messages uses the experimental content-subtype "x-pkcs7-mime" instead of "pkcs7-mime" as it was required by ISIS-MTT 1.0.2. In ISIS-MTT 1.1 this experimental content-subtype MAY be used as well. Thus test step 1 hat to be considered as “passed” with respect version 1.1 of the ISIS-MTT specification.

The failure in test step 4 is due to a failure in test step 16/17 of test case CMS/TCGSD-1 given in the next chapter. This failure in test step 16/17 has to be considered as passed with respect to ISIS-MTT 1.1 as described below. Thus also this test step 4 has to be considered as passed.

4.2 Test Case CMS/TCGSD-1

Date: Mon Jul 5 10:51:02 CEST 2004

Test step 0 (parse ASN.1)	passed
Test step 1 (ContentType)	passed
Test step 2 (Version)	passed

Test step 3 (DigestAlgorithm)	passed
Test step 4 (eContentType)	passed
Test step 5 (eContent)	passed
Test step 6 (Certificates)	passed
Test step 7 (CRLs)	passed
Test step 8 (SignerInfoVersion)	passed
Test step 9 (SignerInfoSID)	passed
Test step 10 (SignerInfoDigestAlgorithm)	passed
Test step 11 (SignerInfoSignedAttributes)	passed
Test step 12/13 (SignerInfoSignedAttributesContentType)	passed
Test step 14/15 (SignerInfoSignedAttributesMessageDigest)	passed
Test step 16/17 (SignerInfoSignedAttributesSigningTime)	failed
Test step 18 (SignerInfoSignatureAlgorithm)	passed
Test step 19 (SignerIngoSignature)	passed
Test step 20 (SignerInfoUnsignedAttributes)	passed
Test step 21/22 (SignerInfoUnsignedAttributesSigningTime)	passed

Test case passed

Note:

In test step 16/17 the ISIS-MTT testbed complains about the encoding of the signing time in UTCTime format which was forbidden in ISIS-MTT 1.0.2 but is now required in ISIS-MTT 1.1. Thus this test step 16/17 has to be considered as passed with respect to version 1.1 of the ISIS-MTT specification.

5 Test Group G-SM/MS

5.1 Test Case TCGSMMS-1

Date: Mon Jul 5 15:21:11 CEST 2004

Test step 1 (Content-Type)	failed
Test step 2 (Boundary of data to be signed)	passed
Test step 3 (Content-Type of MIME entity to be signed)	passed
Test step 4 (Data to be signed)	passed
Test step 5 (Boundary of signature control information)	passed
Test step 6 (Content-Type of signature control information)	failed

Test step 7 (Content-Transfer-Encoding)	passed
Test step 8 (Content-Disposition)	passed
Test step 9 (MIME entity with signed-data)	failed
Test step 10 (Final Boundary)	passed

Test case passed

Notes:

The failures in test step 1 an in test step 6 are due to the fact that Microsoft Outlook when sending S/MIME multipart signed messages uses the experimental content-type "application/x-pkcs7-signature" instead of "application/pkcs7-signature" as it was required by ISIS-MTT 1.0.2. In ISIS-MTT 1.1 this experimental content-type MAY be used as well. Thus test step 1 and test step 6 have to be considered as “passed” with respect to version 1.1 of the ISIS-MTT specification.

The failure in test step 9 is due to a failure in test step 16/17 of test case CMS/TCGSD-3 given in the next chapter. This failure in test step 16/17 has to be considered as passed with respect to ISIS-MTT 1.1 as described below. Thus also this test step 9 has to be considered as passed.

5.2 Test Case CMS/TCGSD-3

Date: Mon Jul 5 15:21:11 CEST 2004

Test step 0 (parse ASN.1)	passed
Test step 1 (ContentType)	passed
Test step 2 (Version)	passed
Test step 3 (DigestAlgorithm)	passed
Test step 4 (eContentType)	passed
Test step 5 (eContent)	passed
Test step 6 (Certificates)	passed
Test step 7 (CRLs)	passed
Test step 8 (SignerInfoVersion)	passed
Test step 9 (SignerInfoSID)	passed
Test step 10 (SignerInfoDigestAlgorithm)	passed
Test step 11 (SignerInfoSignedAttributes)	passed
Test step 12/13 (SignerInfoSignedAttributesContentType)	passed
Test step 14/15 (SignerInfoSignedAttributesMessageDigest)	passed
Test step 16/17 (SignerInfoSignedAttributesSigningTime)	failed
Test step 18 (SignerInfoSignatureAlgorithm)	passed

Test step 19 (SignerIngoSignature)	passed
Test step 20 (SignerInfoUnsignedAttributes)	passed
Test step 21/22 (SignerInfoUnsignedAttributesSigningTime)	passed

Test case passed

Note:

In test step 16/17 the ISIS-MTT testbed complains about the encoding of the signing time in UTCTime format which was forbidden in ISIS-MTT 1.0.2 but is now required in ISIS-MTT 1.1. Thus this test step 16/17 has to be considered as passed with respect to version 1.1 of the ISIS-MTT specification.

6 Test Group P-SM/ED

6.1 Test Case TCPSMED-1

Date: Tue Jul 6 10:25:56 CEST 2004

Test step 1 (Content-Type)	passed
Test step 2 (Content-Transfer-Encoding)	passed
Test step 3 (Content-Disposition)	passed
Test step 4 (MIME entity with enveloped-data)	passed

Test case passed

6.2 Test Case CMS/TCPED-1

Date: Tue Jul 6 10:45:21 CEST 2004

Test step 1 (contentType)	passed
Test step 2 (content.version)	passed
Test step 3 (content.originator-Info)	passed
Test step 4 (content.recipient-Infos)	passed
Test step 5 (content.recipient-Infos.ktri)	passed
Test step 6 (content.recipient-Infos.ktri.version)	passed
Test step 7 (content.recipient-Infos.ktri.rid)	passed
Test step 8 (content.recipient-Infos.ktri .key-EncryptionAlgorithm)	passed
Test step 9 (content.recipient-Infos.ktri.encryptedKey)	passed
Test step 10 (content.encrypted-ContentInfo. contentType)	passed
Test step 11 (content.encrypted-	passed with warning

ContentInfo. contentEncryption-Algorithm)	
Test step 12 (content.encrypted-ContentInfo. encryptedContent)	passed
Test step 13 (content.unprotected-Attrs)	passed

Test case passed with warning

6.3 Test Case INV/TCPSMED-1.1

Date: Tue Jul 6 10:49:08 CEST 2004

Test step 1 (Content-Type)	passed
Test step 2 (Content-Transfer-Encoding)	passed
Test step 3 (Content-Disposition)	passed
Test step 4 (MIME entity with invalid enveloped-data CMS object)	passed

Test case passed

6.4 Test Case INV/CMS/TCPED-1.1

Date: Tue Jul 6 10:52:09 CEST 2004

Test step 1 (contentType)	passed with warning

Test case passed with warning

6.5 Test Case INV/CMS/TCPED-1.2

Date: Tue Jul 6 10:53:32 CEST 2004

Test step 1 (content.version)	passed

Test case passed

6.6 Test Case INV/CMS/TCPED-1.3

Date: Tue Jul 6 10:54:46 CEST 2004

Test step 1 (content.recipient-Infos)	passed

Test case passed

6.7 Test Case INV/CMS/TCPED-1.4

Date: Tue Jul 6 10:56:09 CEST 2004

Test step 1 (content.recipient-Infos.ktri)	passed

Test case passed

6.8 Test Case INV/CMS/TCPED-1.5

Date: Tue Jul 6 10:57:30 CEST 2004

Test step 1 (content.recipient-Infos.ktri.version)	passed

Test case passed

6.9 Test Case INV/CMS/TCPED-1.6

Date: Tue Jul 6 10:58:15 CEST 2004

Test step 1 (content.recipient-Infos.ktri.rid)	passed

Test case passed

6.10 Test Case INV/CMS/TCPED-1.7

Date: Tue Jul 6 10:58:58 CEST 2004

Test step 1 (content.recipient-Infos.ktri.rid)	passed

Test case passed

6.11 Test Case INV/CMS/TCPED-1.8

Date: Tue Jul 6 11:00:51 CEST 2004

Test step 1 (content.recipient-Infos.ktri.key-EncryptionAlgorithm)	passed

Test case passed

6.12 Test Case INV/CMS/TCPED-1.9

Date: Tue Jul 6 11:02:37 CEST 2004

Test step 1 (content.recipient-Infos.ktri.encryptedKey)	passed with warning

Test case passed with warning

6.13 Test Case INV/CMS/TCPED-1.10

Date: Tue Jul 6 11:05:42 CEST 2004

Test step 1 (content.encrypted-ContentInfo.contentType)	passed

Test case passed

6.14 Test Case INV/CMS/TCPED-1.11

Date: Tue Jul 6 11:21:47 CEST 2004

Test step 1 (content.encrypted-ContentInfo.contentEncryption-Algorithm)	passed with warning

Test case passed with warning

6.15 Test Case INV/CMS/TCPED-1.12

Date: Tue Jul 6 11:21:59 CEST 2004

Test step 1 (content.encrypted-ContentInfo.encryptedContent)	passed

Test case passed

7 Test Group P-SM/SD

7.1 Test Case TCPSMSD-1

Date: Tue Jul 6 11:31:17 CEST 2004

Test step 1 (Content-Type)	passed
Test step 2 (Content-Transfer-Encoding)	passed
Test step 3 (Content-Disposition)	passed
Test step 4 (MIME entity with signed-data)	passed

Test case passed

7.2 Test Case CMS/TCPSD-1

Date: Tue Jul 6 11:36:45 CEST 2004

Test step 1 (contentType)	passed
Test step 2 (content.version)	passed

Test step 3 (content.digest-Algorithms)	passed with warning
Test step 4 (content.encap-ContentInfo. eContentType)	passed
Test step 5 (content.encap-ContentInfo.eContent)	passed
Test step 6 (content.certificates)	passed
Test step 7 (content.crls)	passed
Test step 8 (content.signerInfos.version)	passed
Test step 9 (content.signerInfos.sid)	passed
Test step 10 (content.signerInfos.digestAlgorithm)	passed with warning
Test step 11 (content.signerInfos.signedAttrs)	passed
Test step 12 (content.signerInfos.signedAttrs.attrType)	passed
Test step 13 (content.signerInfos.signedAttrs.attrValues)	passed
Test step 14 (content.signerInfos.signedAttrs.attrType)	passed
Test step 15 (content.signerInfos.signedAttrs.attrValues)	passed
Test step 16 (content.signerInfos.signedAttrs.attrType)	passed
Test step 17 (content.signerInfos.signedAttrs.attrValues)	passed
Test step 18 (content.signerInfos.signatureAlgorithm)	passed
Test step 19 (content.signerInfos.signature)	passed
Test step 20 (content.signerInfos.unsignedAttrs)	passed
Test step 21 (content.signerInfos.unsignedAttrs.attrType)	passed
Test step 22 (content.signerInfos.unsignedAttrs.attrValues)	passed

Test case passed with warning

7.3 Test Case INV/TCPSMSD-1.1

Date: Tue Jul 6 12:27:40 CEST 2004

Test step 1 (Content-Type)	passed
Test step 2 (Content-Transfer-Encoding)	passed
Test step 3 (Content-Disposition)	passed
Test step 4 (MIME entity with invalid signed-data CMS object)	passed

Test case passed

7.4 Test Case INV/CMS/TCPSD-1.1

Date: Tue Jul 6 12:29:09 CEST 2004

Test step 1 (contentType)	passed with warning

Test case passed with warning

7.5 Test Case INV/CMS/TCPSD-1.2

Date: Tue Jul 6 12:31:05 CEST 2004

Test step 1 (content.version)	passed

Test case passed

7.6 Test Case INV/CMS/TCPSD-1.3

Date: Tue Jul 6 12:32:00 CEST 2004

Test step 1 (content.digest-Algorithms)	passed with warning

Test case passed with warning

7.7 Test Case INV/CMS/TCPSD-1.4

Date: Tue Jul 6 12:33:39 CEST 2004

Test step 1 (content.encap-ContentInfo.eContentType)	passed

Test case passed

7.8 Test Case INV/CMS/TCPSD-1.5

Date: Tue Jul 6 12:35:25 CEST 2004

Test step 1 (content.encapContentInfo.eContent)	passed

Test case passed

7.9 Test Case INV/CMS/TCPSD-1.6

Date: Tue Jul 6 12:36:38 CEST 2004

Test step 1 (content.certificates)	passed

Test case passed

7.10 Test Case INV/CMS/TCPSD-1.7

Date: Tue Jul 6 12:38:09 CEST 2004

Test step 1 (content.signerInfos)	passed

Test case passed

7.11 Test Case INV/CMS/TCPSD-1.8

Date: Tue Jul 6 12:39:07 CEST 2004

Test step 1 (content.signerInfos.version)	passed

Test case passed

7.12 Test Case INV/CMS/TCPSD-1.9

Date: Tue Jul 6 12:40:33 CEST 2004

Test step 1 (content.signerInfos.sid)	passed

Test case passed

7.13 Test Case INV/CMS/TCPSD-1.10

Date: Tue Jul 6 12:41:42 CEST 2004

Test step 1 (content.signerInfos.sid)	passed

Test case passed

7.14 Test Case INV/CMS/TCPSD-1.11

Date: Tue Jul 6 12:43:22 CEST 2004

Test step 1 (content.signerInfos.digestAlgorithm)	passed

Test case passed

7.15 Test Case INV/CMS/TCPSD-1.12

Date: Tue Jul 6 12:45:10 CEST 2004

Test step 1 (content.signerInfos.signedAttrs)	failed

Test case failed

Note:

When applying this test case, Microsoft Outlook crashes - which indeed has to be rated as “failed”. For the consideration with respect to the ISIS-MTT compliance of the CUT see the corresponding remarks in chapter 1 “Summarized Assessment Results” of this assessment report.

7.16 Test Case INV/CMS/TCPSD-1.13

Date: Tue Jul 6 12:46:44 CEST 2004

Test step 1 (content.signerInfos.signedAttrs.attrType)	passed with warning

Test case passed with warning

7.17 Test Case INV/CMS/TCPSD-1.14

Date: Tue Jul 6 12:48:09 CEST 2004

Test step 1 (content.signerInfos.signedAttrs.attr-Values)	passed with warning

Test case passed with warning

7.18 Test Case INV/CMS/TCPSD-1.15

Date: Tue Jul 6 12:49:16 CEST 2004

Test step 1 (content.signerInfos.signatureAlgorithm)	passed

Test case passed

7.19 Test Case INV/CMS/TCPSD-1.16

Date: Tue Jul 6 12:50:24 CEST 2004

Test step 1 (content.signerInfos.signature)	passed

Test case passed

8 Test Group P-SM/MS

8.1 Test Case TCPSMMS-1

Date: Tue Jul 6 14:06:14 CEST 2004

Test step 1 (Content-Type)	passed

Test step 2 (Boundary (Start of MIME entity to be signed))	passed
Test step 3 (Content-Type)	passed
Test step 4 (Data to be signed)	passed
Test step 5 (Boundary (Start of signature control information))	passed
Test step 6 (Content-Type)	passed
Test step 7 (Content-Transfer-Encoding)	passed
Test step 8 (Content-Disposition)	passed
Test step 9 (MIME entity with signed-data)	passed
Test step 10 (Boundary (end of multi-part/signed message))	passed

Test case passed

8.2 Test Case CMS/TCPSD-3

Date: Tue Jul 6 14:10:59 CEST 2004

Test step 1 (contentType)	passed
Test step 2 (content.version)	passed
Test step 3 (content.digest-Algorithms)	passed with warning
Test step 4 (content.encap-ContentInfo. eContentType)	passed
Test step 5 (content.encap-ContentInfo.eContent)	passed
Test step 6 (content.certificates)	passed
Test step 7 (content.crls)	passed
Test step 8 (content.signerInfos.version)	passed
Test step 9 (content.signerInfos.sid)	passed
Test step 10 (content.signerInfos.digestAlgorithm)	passed with warning
Test step 11 (content.signerInfos.signedAttrs)	passed
Test step 12 (content.signerInfos.signedAttrs.attrType)	passed
Test step 13 (content.signerInfos.signedAttrs.attr-Values)	passed
Test step 14 (content.signerInfos.signedAttrs.attrType)	passed
Test step 15 (content.signerInfos.signedAttrs.attr-Values)	passed
Test step 16 (content.signerInfos.signedAttrs.attrType)	passed
Test step 17 (content.signerInfos.signedAttrs.attr-Values)	passed
Test step 18 (content.signerInfos.signatureAlgorithm)	passed
Test step 19 (content.signerInfos.signature)	passed

Test step 20 (content.signerInfos.unsignedAttrs)	passed
Test step 21 (content.signerInfos.unsignedAttrs.attr-Type)	passed
Test step 22 (content.signerInfos.unsignedAttrs.attr-Values)	passed

Test case passed with warning

8.3 Test Case INV/TCPSMMS-1.1

Date: Tue Jul 6 14:12:50 CEST 2004

Test step 1 (Content-Type)	passed
Test step 2 (Boundary (Start of MIME entity to be signed))	passed
Test step 3 (Content-Type)	passed
Test step 4 (Data to be signed)	passed
Test step 5 (Boundary (Start of signature control information))	passed
Test step 6 (Content-Type)	passed
Test step 7 (Content-Transfer-Encoding)	passed
Test step 8 (Content-Disposition)	passed
Test step 9 (MIME entity with invalid signed-data CMS object)	passed
Test step 10 (Boundary (end of multipart/signed message))	passed

Test case passed

8.4 Test Case INV/CMS/TCPSD-3.1

Date: Tue Jul 6 14:13:28 CEST 2004

Test step 1 (contentType)	passed with warning

Test case passed with warning

8.5 Test Case INV/CMS/TCPSD-3.2

Date: Tue Jul 6 14:14:23 CEST 2004

Test step 1 (content.version)	passed

Test case passed

8.6 Test Case INV/CMS/TCPSD-3.3

Date: Tue Jul 6 14:15:17 CEST 2004

Test step 1 (content.digest-Algorithms)	passed with warning

Test case passed with warning

8.7 Test Case INV/CMS/TCPSD-3.4

Date: Tue Jul 6 14:16:12 CEST 2004

Test step 1 (content.encap-ContentInfo.eContentType)	passed

Test case passed

8.8 Test Case INV/CMS/TCPSD-3.5

Date: Tue Jul 6 14:17:43 CEST 2004

Test step 1 (content.encap-ContentInfo.eContent)	passed

Test case passed

8.9 Test Case INV/CMS/TCPSD-3.6

Date: Tue Jul 6 14:18:45 CEST 2004

Test step 1 (content.signerInfos.version)	passed

Test case passed

8.10 Test Case INV/CMS/TCPSD-3.7

Date: Tue Jul 6 14:19:42 CEST 2004

Test step 1 (content.signerInfos.sid)	passed with warning

Test case passed with warning

8.11 Test Case INV/CMS/TCPSD-3.8

Date: Tue Jul 6 14:21:08 CEST 2004

Test step 1 (content.signerInfos.sid)	passed

Test case passed

8.12 Test Case INV/CMS/TCPSD-3.9

Date: Tue Jul 6 14:22:01 CEST 2004

Test step 1 (content.signerInfos.digestAlgorithm)	passed

Test case passed

8.13 Test Case INV/CMS/TCPSD-3.10

Date: Tue Jul 6 14:22:52 CEST 2004

Test step 1 (content.signerInfos.digestAlgorithm)	passed

Test case passed

8.14 Test Case INV/CMS/TCPSD-3.11

Date: Tue Jul 6 14:23:39 CEST 2004

Test step 1 (content.signerInfos.signedAttrs)	failed

Test case failed

Note:

When applying this test case, Microsoft Outlook crashes - which indeed has to be rated as “failed”. For the consideration with respect to the ISIS-MTT compliance of the CUT see the corresponding remarks in chapter 1 “Summarized Assessment Results” of this assessment report.

8.15 Test Case INV/CMS/TCPSD-3.12

Date: Tue Jul 6 14:25:30 CEST 2004

Test step 1 (content.signerInfos.signedAttrs.attrValues)	passed

Test case passed

8.16 Test Case INV/CMS/TCPSD-3.13

Date: Tue Jul 6 14:26:23 CEST 2004

Test step 1 (content.signerInfos.signedAttrs)	passed with warning

Test case passed with warning

8.17 Test Case INV/CMS/TCPSD-3.14

Date: Tue Jul 6 14:27:28 CEST 2004

Test step 1 (content.signerInfos.signedAttrs)	passed with warning

Test case passed with warning

8.18 Test Case INV/CMS/TCPSD-3.15

Date: Tue Jul 6 14:29:31 CEST 2004

Test step 1 (content.signerInfos.signedAttrs.attrValues)	passed

Test case passed

8.19 Test Case INV/CMS/TCPSD-3.16

Date: Tue Jul 6 14:30:33 CEST 2004

Test step 1 (content.signerInfos.signedAttrs)	passed with warning

Test case passed with warning

8.20 Test Case INV/CMS/TCPSD-3.17

Date: Tue Jul 6 14:31:20 CEST 2004

Test step 1 (content.signerInfos.signedAttrs.attrValues)	passed with warning

Test case passed with warning

8.21 Test Case INV/CMS/TCPSD-3.18

Date: Tue Jul 6 14:32:59 CEST 2004

Test step 1 (content.signerInfos.signatureAlgorithm)	passed

Test case passed

8.22 Test Case INV/CMS/TCPSD-3.19

Date: Tue Jul 6 14:33:50 CEST 2004

Test step 1 (content.signerInfos.signature)	passed

Test case passed

9 Test Group PATHVALID

9.1 Test Case VALID/TCPVVALID-1

Date: Tue Jul 6 13:48:54 CEST 2004

Test step 1 (BuildAndValidateCertPath())	passed

Test case passed

9.2 Test Case INVALID/TCPVSIGINVALID-1

Date: Tue Jul 6 13:52:17 CEST 2004

Test step 1 (ValidateCertPath())	passed
Test step 2 (BuildAndValidateCertPath())	passed

Test case passed

9.3 Test Case INVALID/TCPVSIGINVALID-2

Date: Tue Jul 6 13:54:09 CEST 2004

Test step 1 (ValidateCertPath())	passed
Test step 2 (BuildAndValidateCertPath())	passed

Test case passed

9.4 Test Case INVALID/TCPVCERTREVO-1

Date: Tue Jul 6 13:56:07 CEST 2004

Test step 1 (CheckStatusUsingCRL())	passed
Test step 2 (CheckRevocationStatus())	passed
Test step 3 (ValidateCertPath())	passed
Test step 4 (BuildAndValidateCertPath())	passed

Test case passed

9.5 Test Case INVALID/TCPVEXPIRED-1

Date: Tue Jul 6 13:56:46 CEST 2004

Test step 1 (ValidateCertPath())	passed

Test step 2 (BuildAndValidateCertPath())	passed

Test case passed

9.6 Test Case INVALID/TCPVINVALIDCA-1

Date: Tue Jul 6 14:00:51 CEST 2004

Test step 1 (ValidateCertPath())	passed
Test step 2 (BuildAndValidateCertPath())	passed

Test case passed

10 Technical Data

The following products have been used in this assessment:

- Windows XP Professional Version 2002 SP1
- Microsoft Office Outlook 2003
- DATEV SmartCard Sicherheitspaket V1.41 including
  - SmartCard-Windows-Integration V1.1 including
    - DATEVe:secure MAIL V1.1

11 Test Procedure

11.1 Installation and Configuration

On one system the components required for the e-mail client were installed, namely

- Windows XP Professional Version 2002 SP1
  (German, including Microsoft Internet Explorer 6.0)
- Microsoft Office Outlook 2003 (German)
- a PC/SC compatible smartcard reader (Chipdrive extern USB)
- DATEV SmartCard Sicherheitspaket V1.41 (including DATEVe:secure MAIL V.1.1) including a DATEV-SmartCard classic
  with keys and certificates supplied by the DATEV trust center

All components were installed with standard (typical and/or default) configuration and without any additional patches.

The EE and CA certificates stored on the smartcard were exported using a DATEV smartcard utility and imported in the Windows certificate store. In particular the DATEV CA certificate was installed as a trustworthy root certificate.

The certificates of the ISIS-MTT testbed certificate chain used for S/MIME encryption generation and signature processing tests were also imported in the Windows certificate store. A new contact was created in the Outlook e-mail client and associated with the appropriate ISIS-MTT testbed EE certificate.

On another system the ISIS-MTT Testbed 1.1 Build 5 SP 1 was installed with the following modifications:

- The CUT uses a processor based smartcard for the secure storage and handling of the users private key. It is not possible to replace this key e.g. with the private key provided by the testbed for conducting the S/MIME signature generation and encryption processing tests. Therefore the testbed was modified to allow a given user certificate to be used for these tests.
- Some test e-mails provided by the testbed for testing the processing of multipart-signed messages contained spurious additional data bytes trailing the CMS message. These test messages were corrected.

11.2 Performing the Tests

The components

- DATEVe:secure MAIL and
- Microsoft Office Outlook 2003

in combination comprise the CUT that was subjected to the ISIS-MTT compliance assessment with respect to the ISIS-MTT product class “E-Mail Client”.

The CUT uses the certificate store of the underlying Microsoft Windows operating system.

The test cases for Part 1 “Certificate and CRL Profile” and Part 5 “Certificate Path Validation” were performed using the certificate management tools embedded in the Windows operating system.

Test case TCPVCERTREVO-1 - also belonging to Part 5 - could not be covered this way. It was performed by sending the Outlook e-mail client a manually prepared e-mail signed with the revoked EE certificate in order to enforce an evaluation of the corresponding CRL.

The test cases for Part 3 “Message Formats” were performed using the Microsoft Office Outlook 2003 e-mail client, which in turn used the underlying security components provided by DATEVe:secure MAIL.

12 Component Conformance Statement

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER				
REFERENCE NUMBER				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
	Generation and processing of certificates and CRLS			
1	Generation of public key certificates	☐	☒	
2	Generation of attribute certificates	☐	☒	
3	Generation of cross certificates	☐	☒	
4	Generation of CRLs	☐	☒	
5	Processing of public key certificates	☒	☐	
6	Processing of attribute certificates	☐	☒	
7	Processing of cross certificates	☐	☒	
8	Processing of CRLs	☒	☐	
	CMC			
9	“Simple CMC” in EEs	☐	☒	
10	“Simple CMC” in CAs	☐	☒	
	Generation and processing of S/MIME messages			
11	Generation of an S/MIME Message for Enveloped Data	☒	☐	
12	Generation of an S/MIME Message for Signed Data	☒	☐	
13	Generation of an S/MIME Message for Transporting Certificates in Certification Responses	☐	☒	
14	Generation of a Multipart/Signed S/MIME Message	☒	☐	
15	Processing of a S/MIME message for enveloped-data	☒	☐	
16	Processing of S/MIME messages with signed data	☒	☐	
17	Processing of a valid S/MIME message for transporting certificates in certification responses (certs-only)	☐	☒	
18	Processing of a Multipart/Signed S/MIME message	☒	☐	
19	File signature and encryption	☐	☒	
20	**LDAP**			

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER				
REFERENCE NUMBER				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
21	LDAP client	☒	☐	
22	LDAP server	☐	☒	
	OCSP-Clients and Servers			
23	Transport of an OCSP Request	☐	☒	
24	Retrieval of OCSP responses	☐	☒	
25	Retrieval of an OCSP request	☐	☒	
26	Transport of an OCSP response	☐	☒	
	TSP			
27	TSP client	☐	☒	
28	TSP server	☐	☒	
	Certificate path validation			
29	Processing of a valid, 3-step certificate path	☒	☐	
30	Processing of an invalid certificate path	☒	☐	
	ISIS-MTT SigG-Profile			
31	Generation of SigG-conforming PKCs	☐	☒	
32	Generation of SigG-conforming ACs	☐	☒	
33	Processing of SigG-conforming PKC	☐	☒	
34	Processing of SigG-conforming ACs	☐	☒	
35	Generation of an OCSP Response of SigG-conforming client	☐	☒	
36	Processing of an OCSP Response of a SigG-conforming OCSP-server	☐	☒	
	PKCS#11			
37	PKCS#11 general functions	☐	☒	
38	PKCS#11 functions for slot- and token management	☐	☒	
39	PKCS#11 functions for session management	☐	☒	
40	PKCS#11 functions for session management – optional functions	☐	☒	
41	PKCS#11 functions for object management	☐	☒	

CONFORMANCE CLAIMS OF COMPONENTS UNDER TEST (MANUFACTURERS) REGARDING THE FUNCTIONALITY CLASSES OF PRODUCTS				
PRODUCT AND MANUFACTURER				
REFERENCE NUMBER				
FUNCTIONALITY CLASSES		CLAIMED SUPPORT		
#	NAME	YES	NO	REMARKS
42	PKCS#11 functions for encryption	☐	☒	
43	PKCS#11 functions for decryption	☐	☒	
44	PKCS#11 functions for message digesting	☐	☒	
45	PKCS#11 functions for signing	☐	☒	
46	PKCS#11 functions for signing – optional functions	☐	☒	
47	PKCS#11 functions for verification	☐	☒	
48	PKCS#11 functions for verification – optional functions	☐	☒	
49	PKCS#11 functions for combined cryptographic operations	☐	☒	
50	PKCS#11 functions for combined cryptographic operations – optional functions	☐	☒	
51	PKCS#11 functions for key management	☐	☒	
52	PKCS#11 functions for generation of random numbers	☐	☒	
53	PKCS#11 functions for parallel functions management	☐	☒	
54	PKCS#11 functions for stubs	☐	☒	

13 Annex I: Test Log

13.1 FC5: Processing of public key certificates

Starting Test Session for: Fritz Bauspiess

Date: Wed Jun 30 14:46:33 CEST 2004

Component Under Test

Manufacturer: DATEV eG

Product Name: DATEVe:secure MAIL

Version: V.1.1

Starting test case TCPPKC-1

Date: Wed Jun 30 15:36:08 CEST 2004

Test step 1 (Certificate) -- passed

Test step 2 (signatureAlgorithm) -- passed with warning

Remarks: Test of algorithm "RSA with RIPEMD" fails, because RIPEMD is not supported. Requirement for RIPEMD is reduced to "SHOULD" in ISIS-MTT 1.1.

Test step 3 (signature) -- passed

Test step 4 (version) -- passed

Test step 5 (serialNumber) -- passed

Test step 6 (issuer) -- passed with warning

Remarks: DName extension "businessCategory" (OID 2.5.4.15) (ISIS-MTT: "SHOULD") unknown. Parsing of remaining DName extensions undisturbed.

Test step 7 (validity) -- passed

Test step 8 (subject) -- passed with warning

Remarks: The following DName extensions are only recognized by their OID, not by their name, but parsing is ok for all DName extensions.

MUST extensions: nameAtBirth(1.3.36.8.3.14), countryOfResidence(1.3.6.1.5.5.7.9.5), countryOfCitizenship(1.3.6.1.5.5.7.9.4), gender(1.3.6.1.5.5.7.9.3), placeOfBirth(1.3.6.1.5.5.7.9.2), pseudonym(2.5.4.65)

SHOULD extensions: generationQualifier(2.5.4.44), businessCategory(2.5.4.15)

Test step 9 (subjectPublicKeyInfo) -- passed

Test step 10 (issuerUniqueID) -- passed

Test step 11 (subjectUniqueID) -- passed

Test step 12 (extensions) -- passed with warning

Remarks: All MUST extensions recognized.

The following SHOULD extensions were not recognized but parsing went ok: OCSPNoCheck(1.3.6.1.5.5.7.48.1.5), BiometricInfo(1.3.6.1.5.5.7.1.2), QCStatements(1.3.6.1.5.5.7.1.3), SubjectDirectoryAttributes(2.5.29.9)

End of test case TCPPKC-1

Test case passed with warning

Date: Wed Jun 30 15:36:08 CEST 2004

13.2 FC8: Processing of CRLs

Starting Test Session for: Fritz Bauspiess

Date: Wed Jun 30 15:39:00 CEST 2004

Component Under Test

Manufacturer: DATEV eG

Product Name: DATEVe:secure MAIL

Version: V.1.1

Starting test case TCPCRL-1

Date: Wed Jun 30 16:04:04 CEST 2004

Test step 1 (CertificateList) -- passed

Test step 2 (signatureAlgorithm) -- passed with warning

Remarks: Test of algorithm "RSA with RIPEMD" fails, because RIPEMD is not supported. Requirement for RIPEMD is reduced to "SHOULD" in ISIS-MTT 1.1.

Test step 3 (signatureValue) -- passed

Test step 4 (issuer) -- passed with warning

Remarks: DName extension "businessCategory" (OID 2.5.4.15) (ISIS-MTT: "SHOULD") unknown. Parsing of remaining DName extensions undisturbed.

Test step 5 (thisUpdate) -- passed

Test step 6 (nextUpdate) -- passed

Test step 7 (revokedCertificates) -- passed

Test step 7 a) (userCertificate) -- passed

Test step 7 b) (revocationDate) -- passed

Test step 7 c) (crlEntryExtensions) -- passed with warning

Remarks: caIssuer (OID 2.5.29.29), i.e. indirect CRLs, not supported although correctly parsed. Support requirement reduced from "MUST" to "SHOULD" according to a corresponding decision of the ISIS-MTT-Board as of May 27th, 2004.

HoldInstructionCode(OID 2.5.29.23)(ISIS-MTT: "SHOULD") not recognized but correctly parsed.

Test step 8 (crlExtensions) -- passed

End of test case TCPCRL-1

Test case passed with warning

Date: Wed Jun 30 16:04:04 CEST 2004

13.3 FC11: Generation of an S/MIME Message for Enveloped Data

Starting Test Session for: Fritz Bauspiess

Date: Mon Jul 5 10:30:36 CEST 2004

Component Under Test

Manufacturer: DATEV eG

Product Name: DATEVe:secure MAIL

Version: 1.1

Starting test case TCGSMED-1

Date: Mon Jul 5 10:32:35 CEST 2004

Test step 1 (Content-Type) -- failed

Remarks: Content-Subtype is "x-pkcs7-mime" instead of "pkcs7-mime"

Test step 2 (Content-Transfer-Encoding) -- passed

Test step 3 (Content-Disposition) -- passed

Test step 4 (MIME entity with enveloped-data) --

Starting test case TCGED-1

Date: Mon Jul 5 10:32:35 CEST 2004

Test step 0 (parse ASN.1) -- passed

Test step 1 (ContentType) -- passed

Test step 2 (Version) -- passed

Test step 3 (OriginatorInfo) -- passed

Test step 4 (RecipientInfos) -- passed

Test step 5 (KeyTransRecipientInfo (ktri)) -- passed
Test step 6 (ktriVersion) -- passed
Test step 7 (ktriRecipientIdentifier) -- passed
Remarks: RecipientIdentifier certificate serial number is "19"
Test step 8 (ktriKeyEncryptionAlgorithm) -- passed
Remarks: Algorithm is "rsaEncryption"
Test step 9 (ktriEncryptedKey) -- passed
Test step 10 (EncryptedContentInfoContentType) -- passed
Test step 11 (EncryptedContentInfoEncryptionAlgorithm) -- passed
Remarks: Algorithm is "des-EDE3-CBC"
Test step 12 (EncryptedContentInfoEncryptedContent) -- passed
Test step 13 (UnprotectedAttributes) -- passed
End of test case TCGED-1
Test case passed
Date: Mon Jul 5 10:32:36 CEST 2004

passed
End of test case TCGSMED-1
Test case failed
Date: Mon Jul 5 10:32:36 CEST 2004

13.4 FC12: Generation of an S/MIME Message for Signed Data

Starting Test Session for: Fritz Bauspiess

Date: Mon Jul 5 10:45:58 CEST 2004

Component Under Test
Manufacturer: DATEV eG
Product Name: DATEVe:secure MAIL
Version: 1.1

Starting test case TCGSMSD-1
Date: Mon Jul 5 10:51:02 CEST 2004
Test step 1 (Content-Type) -- failed

Remarks: Content-Subtype is "x-pkcs7-mime" instead of "pkcs7-mime"
Test step 2 (Content-Transfer-Encoding) -- passed
Test step 3 (Content-Disposition) -- passed
Test step 4 (MIME entity with signed-data) --

Starting test case TCGSD-1
Date: Mon Jul 5 10:51:02 CEST 2004
Test step 0 (parse ASN.1) -- passed
Test step 1 (ContentType) -- passed
Test step 2 (Version) -- passed
Remarks: Version is "1"
Test step 3 (DigestAlgorithm) -- passed
Test step 4 (eContentType) -- passed
Test step 5 (eContent) -- passed
Test step 6 (Certificates) -- passed
Remarks: Certificate set is complete
Test step 7 (CRLs) -- passed
Remarks: No CRLs found
Test step 8 (SignerInfoVersion) -- passed
Test step 9 (SignerInfoSID) -- passed
Remarks: SerialNumber is "0x018AED049B"
Test step 10 (SignerInfoDigestAlgorithm) -- passed
Remarks: Algorithm is "sha1"
Test step 11 (SignerInfoSignedAttributes) -- passed
Test step 12/13 (SignerInfoSignedAttributesContentType) -- passed
Test step 14/15 (SignerInfoSignedAttributesMessageDigest) -- passed
Test step 16/17 (SignerInfoSignedAttributesSigningTime) -- failed
Remarks: Wrong encoding "UTCTime"
Test step 18 (SignerInfoSignatureAlgorithm) -- passed
Test step 19 (SignerIngoSignature) -- passed
Test step 20 (SignerInfoUnsignedAttributes) -- passed
Remarks: No UnsignedAttributes found
Test step 21/22 (SignerInfoUnsignedAttributesSigningTime) -- passed
Remarks: No UnsignedAttributes found
End of test case TCGSD-1

Test case failed
Date: Mon Jul 5 10:51:03 CEST 2004

failed
End of test case TCGSMSD-1
Test case failed
Date: Mon Jul 5 10:51:03 CEST 2004

13.5 FC14: Generation of a Multipart/Signed S/MIME Message

Starting Test Session for: Fritz Bauspiess

Date: Mon Jul 5 15:19:16 CEST 2004

Component Under Test
Manufacturer: DATEV eG
Product Name: DATEVe:secure MAIL
Version: 1.1

Starting test case TCGSMMS-1
Date: Mon Jul 5 15:21:11 CEST 2004
Test step 1 (Content-Type) -- failed
Remarks: Protocol is "application/x-pkcs7-signature" instead of "application/pkcs7-signature"
Test step 2 (Boundary of data to be signed) -- passed
Test step 3 (Content-Type of MIME entity to be signed) -- passed
Test step 4 (Data to be signed) -- passed
Test step 5 (Boundary of signature control information) -- passed
Test step 6 (Content-Type of signature control information) -- failed
Remarks: Content-Type is "application/x-pkcs7-signature"
Test step 7 (Content-Transfer-Encoding) -- passed
Test step 8 (Content-Disposition) -- passed
Test step 9 (MIME entity with signed-data) --

Starting test case TCGSD-3
Date: Mon Jul 5 15:21:11 CEST 2004

Test step 0 (parse ASN.1) -- passed
Test step 1 (ContentType) -- passed
Test step 2 (Version) -- passed
Remarks: Version is "1"
Test step 3 (DigestAlgorithm) -- passed
Test step 4 (eContentType) -- passed
Test step 5 (eContent) -- passed
Test step 6 (Certificates) -- passed
Remarks: Certificate set is complete
Test step 7 (CRLs) -- passed
Remarks: No CRLs found
Test step 8 (SignerInfoVersion) -- passed
Test step 9 (SignerInfoSID) -- passed
Remarks: SerialNumber is "0x018AED049B"
Test step 10 (SignerInfoDigestAlgorithm) -- passed
Remarks: Algorithm is "sha1"
Test step 11 (SignerInfoSignedAttributes) -- passed
Test step 12/13 (SignerInfoSignedAttributesContentType) -- passed
Test step 14/15 (SignerInfoSignedAttributesMessageDigest) -- passed
Test step 16/17 (SignerInfoSignedAttributesSigningTime) -- failed
Remarks: Wrong encoding "UTCTime"
Test step 18 (SignerInfoSignatureAlgorithm) -- passed
Test step 19 (SignerIngoSignature) -- passed
Test step 20 (SignerInfoUnsignedAttributes) -- passed
Remarks: No UnsignedAttributes found
Test step 21/22 (SignerInfoUnsignedAttributesSigningTime) -- passed
Remarks: No UnsignedAttributes found
End of test case TCGSD-3
Test case failed
Date: Mon Jul 5 15:21:12 CEST 2004

failed
Test step 10 (Final Boundary) -- passed
End of test case TCGSMMS-1
Test case failed

Date: Mon Jul 5 15:21:12 CEST 2004

13.6 FC15: Processing of an S/MIME Message for Enveloped Data

Starting Test Session for: Fritz Bauspiess

Date: Tue Jul 6 10:21:53 CEST 2004

Component Under Test
Manufacturer: DATEV eG
Product Name: DATEVe:secure MAIL
Version: 1.1

Starting test case TCPSMED-1
Date: Tue Jul 6 10:25:56 CEST 2004
Test step 1 (Content-Type) -- passed
Test step 2 (Content-Transfer-Encoding) -- passed
Test step 3 (Content-Disposition) -- passed
Test step 4 (MIME entity with enveloped-data) -- passed
End of test case TCPSMED-1
Test case passed
Date: Tue Jul 6 10:25:56 CEST 2004

Starting test case TCPED-1
Date: Tue Jul 6 10:45:21 CEST 2004
Test step 1 (contentType) -- passed
Test step 2 (content.version) -- passed
Test step 3 (content.originator-Info) -- passed
Test step 4 (content.recipient-Infos) -- passed
Test step 5 (content.recipient-Infos.ktri) -- passed
Test step 6 (content.recipient-Infos.ktri.version) -- passed
Test step 7 (content.recipient-Infos.ktri.rid) -- passed
Test step 8 (content.recipient-Infos.ktri .key-EncryptionAlgorithm) -- passed
Remarks: RSA-PKCS1-v1_5 supported, RSAES-OAEP not supported but only marked as "+-" (=MAY) in ISIS-MTT 1.1

Test step 9 (content.recipient-Infos.ktri.encryptedKey) -- passed

Test step 10 (content.encrypted-ContentInfo. contentType) -- passed

Test step 11 (content.encrypted-ContentInfo.
contentEncryption-Algorithm) -- passed with warning

Remarks: DES-CBC and DES-EDE3-CBC supported, DES3-CBC not supported and marked as "+" (=SHOULD) in ISIS-MTT 1.1

Test step 12 (content.encrypted-ContentInfo.
encryptedContent) -- passed

Test step 13 (content.unprotected-Attrs) -- passed

End of test case TCPED-1

Test case passed with warning

Date: Tue Jul 6 10:45:21 CEST 2004

Starting Test Session for: Fritz Bauspiess

Date: Tue Jul 6 10:47:12 CEST 2004

Component Under Test

Manufacturer: DATEV eG

Product Name: DATEVe:secure MAIL

Version: 1.1

Starting test case TCPSMED-1.1

Date: Tue Jul 6 10:49:08 CEST 2004

Test step 1 (Content-Type) -- passed

Test step 2 (Content-Transfer-Encoding) -- passed

Test step 3 (Content-Disposition) -- passed

Test step 4 (MIME entity with invalid enveloped-data CMS object) -- passed

End of test case TCPSMED-1.1

Test case passed

Date: Tue Jul 6 10:49:08 CEST 2004

Starting test case TCPED-1.1

Date: Tue Jul 6 10:52:09 CEST 2004

Test step 1 (contentType) -- passed with warning

Remarks: missleading error message but processing is ok

End of test case TCPED-1.1

Test case passed with warning

Date: Tue Jul 6 10:52:09 CEST 2004

Starting test case TCPED-1.2

Date: Tue Jul 6 10:53:32 CEST 2004

Test step 1 (content.version) -- passed

Remarks: illegal content of field is ignored, message is processed correctly

End of test case TCPED-1.2

Test case passed

Date: Tue Jul 6 10:53:32 CEST 2004

Starting test case TCPED-1.3

Date: Tue Jul 6 10:54:46 CEST 2004

Test step 1 (content.recipient-Infos) -- passed

End of test case TCPED-1.3

Test case passed

Date: Tue Jul 6 10:54:46 CEST 2004

Starting test case TCPED-1.4

Date: Tue Jul 6 10:56:09 CEST 2004

Test step 1 (content.recipient-Infos.ktri) -- passed

End of test case TCPED-1.4

Test case passed

Date: Tue Jul 6 10:56:09 CEST 2004

Starting test case TCPED-1.5

Date: Tue Jul 6 10:57:30 CEST 2004

Test step 1 (content.recipient-Infos.ktri.version) -- passed

Remarks: illegal version ignored, message processed correctly

End of test case TCPED-1.5

Test case passed

Date: Tue Jul 6 10:57:30 CEST 2004

Starting test case TCPED-1.6

Date: Tue Jul 6 10:58:15 CEST 2004

Test step 1 (content.recipient-Infos.ktri.rid) -- passed

End of test case TCPED-1.6

Test case passed

Date: Tue Jul 6 10:58:15 CEST 2004

Starting test case TCPED-1.7

Date: Tue Jul 6 10:58:58 CEST 2004

Test step 1 (content.recipient-Infos.ktri.rid) -- passed

End of test case TCPED-1.7

Test case passed

Date: Tue Jul 6 10:58:58 CEST 2004

Starting test case TCPED-1.8

Date: Tue Jul 6 11:00:51 CEST 2004

Test step 1 (content.recipient-Infos.ktri.key-EncryptionAlgorithm) -- passed

Remarks: invalid OID ignored, algorithm info is retrieved elsewhere, processing is ok

End of test case TCPED-1.8

Test case passed

Date: Tue Jul 6 11:00:51 CEST 2004

Starting test case TCPED-1.9

Date: Tue Jul 6 11:02:37 CEST 2004

Test step 1 (content.recipient-Infos.ktri.encryptedKey) -- passed with warning

Remarks: missleading error message, but processing ok

End of test case TCPED-1.9

Test case passed with warning

Date: Tue Jul 6 11:02:37 CEST 2004

Starting test case TCPED-1.10

Date: Tue Jul 6 11:05:42 CEST 2004

Test step 1 (content.encrypted-ContentInfo.contentType) -- passed

Remarks: unknown content type detected, message is represented and correctly decrypted as an attachment to the user

End of test case TCPED-1.10

Test case passed

Date: Tue Jul 6 11:05:42 CEST 2004

Starting test case TCPED-1.11

Date: Tue Jul 6 11:21:47 CEST 2004

Test step 1 (content.encrypted-ContentInfo.contentEncryption-Algorithm) -- passed with warning

Remarks: missleading error message, but processing is ok

End of test case TCPED-1.11

Test case passed with warning

Date: Tue Jul 6 11:21:47 CEST 2004

Starting test case TCPED-1.12

Date: Tue Jul 6 11:21:59 CEST 2004

Test step 1 (content.encrypted-ContentInfo.encryptedContent) -- passed

End of test case TCPED-1.12

Test case passed

Date: Tue Jul 6 11:21:59 CEST 2004

13.7 FC16: Processing of S/MIME Messages with signed data

Starting Test Session for: Fritz Bauspiess

Date: Tue Jul 6 11:28:31 CEST 2004

Component Under Test

Manufacturer: DATEV eG

Product Name: DATEVe:secure MAIL

Version: 1.1

Starting test case TCPSMSD-1

Date: Tue Jul 6 11:31:17 CEST 2004

Test step 1 (Content-Type) -- passed

Test step 2 (Content-Transfer-Encoding) -- passed

Test step 3 (Content-Disposition) -- passed

Test step 4 (MIME entity with signed-data) -- passed
End of test case TCPSMSD-1
Test case passed
Date: Tue Jul 6 11:31:17 CEST 2004

Starting test case TCPSD-1
Date: Tue Jul 6 11:36:45 CEST 2004
Test step 1 (contentType) -- passed
Test step 2 (content.version) -- passed
Test step 3 (content.digest-Algorithms) -- passed with warning
Remarks: RIPEMD-160 not supported but marked as "+" (=SHOULD) in ISISMTT 1.1
Test step 4 (content.encap-ContentInfo. eContentType) -- passed
Test step 5 (content.encap-ContentInfo.eContent) -- passed
Test step 6 (content.certificates) -- passed
Test step 7 (content.crls) -- passed
Test step 8 (content.signerInfos.version) -- passed
Test step 9 (content.signerInfos.sid) -- passed
Test step 10 (content.signerInfos.digestAlgorithm) -- passed with warning
Remarks: RIPEMD-160 not supported but marked as "+" (=SHOULD) in ISISMTT 1.1
Test step 11 (content.signerInfos.signedAttrs) -- passed
Test step 12 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 13 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 14 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 15 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 16 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 17 (content.signerInfos.signedAttrs.attrValues) -- passed
Test step 18 (content.signerInfos.signatureAlgorithm) -- passed
Test step 19 (content.signerInfos.signature) -- passed
Test step 20 (content.signerInfos.unsignedAttrs) -- passed
Test step 21 (content.signerInfos.unsignedAttrs.attrType) -- passed
Test step 22 (content.signerInfos.unsignedAttrs.attrValues) -- passed
End of test case TCPSD-1
Test case passed with warning
Date: Tue Jul 6 11:36:45 CEST 2004

Starting Test Session for: Fritz Bauspiess

Date: Tue Jul 6 12:25:57 CEST 2004

Component Under Test
Manufacturer: DATEV eG
Product Name: DATEVe:secure MAIL
Version: 1.1

Starting test case TCPSMSD-1.1
Date: Tue Jul 6 12:27:40 CEST 2004

Test step 1 (Content-Type) -- passed
Test step 2 (Content-Transfer-Encoding) -- passed
Test step 3 (Content-Disposition) -- passed
Test step 4 (MIME entity with invalid signed-data CMS object) -- passed
End of test case TCPSMSD-1.1
Test case passed
Date: Tue Jul 6 12:27:40 CEST 2004

Starting test case TCPSD-1.1
Date: Tue Jul 6 12:29:09 CEST 2004
Test step 1 (contentType) -- passed with warning
Remarks: missleading error message but processing is ok
End of test case TCPSD-1.1
Test case passed with warning
Date: Tue Jul 6 12:29:09 CEST 2004

Starting test case TCPSD-1.2
Date: Tue Jul 6 12:31:05 CEST 2004
Test step 1 (content.version) -- passed
Remarks: illegal version ignored, message processed correctly
End of test case TCPSD-1.2
Test case passed
Date: Tue Jul 6 12:31:05 CEST 2004

Starting test case TCPSD-1.3
Date: Tue Jul 6 12:32:00 CEST 2004
Test step 1 (content.digest-Algorithms) -- passed with warning
Remarks: missleading error message but processing is ok
End of test case TCPSD-1.3
Test case passed with warning
Date: Tue Jul 6 12:32:00 CEST 2004

Starting test case TCPSD-1.4
Date: Tue Jul 6 12:33:39 CEST 2004
Test step 1 (content.encap-ContentInfo.eContentType) -- passed
Remarks: message presented and decoded as attachment
End of test case TCPSD-1.4
Test case passed
Date: Tue Jul 6 12:33:39 CEST 2004

Starting test case TCPSD-1.5
Date: Tue Jul 6 12:35:25 CEST 2004
Test step 1 (content.encapContentInfo.eContent) -- passed
Remarks: modification detected correctly, invalid signature signaled
End of test case TCPSD-1.5
Test case passed
Date: Tue Jul 6 12:35:25 CEST 2004

Starting test case TCPSD-1.6
Date: Tue Jul 6 12:36:38 CEST 2004
Test step 1 (content.certificates) -- passed
Remarks: message decoded correctly
End of test case TCPSD-1.6
Test case passed
Date: Tue Jul 6 12:36:38 CEST 2004

Starting test case TCPSD-1.7
Date: Tue Jul 6 12:38:09 CEST 2004

Test step 1 (content.signerInfos) -- passed

Remarks: error in signerInfos signaled, message decoded correctly

End of test case TCPSD-1.7

Test case passed

Date: Tue Jul 6 12:38:09 CEST 2004

Starting test case TCPSD-1.8

Date: Tue Jul 6 12:39:07 CEST 2004

Test step 1 (content.signerInfos.version) -- passed

Remarks: illegal version ignored, message decoded correctly

End of test case TCPSD-1.8

Test case passed

Date: Tue Jul 6 12:39:07 CEST 2004

Starting test case TCPSD-1.9

Date: Tue Jul 6 12:40:33 CEST 2004

Test step 1 (content.signerInfos.sid) -- passed

End of test case TCPSD-1.9

Test case passed

Date: Tue Jul 6 12:40:33 CEST 2004

Starting test case TCPSD-1.10

Date: Tue Jul 6 12:41:42 CEST 2004

Test step 1 (content.signerInfos.sid) -- passed

Remarks: invalid certificate detected and signaled

End of test case TCPSD-1.10

Test case passed

Date: Tue Jul 6 12:41:42 CEST 2004

Starting test case TCPSD-1.11

Date: Tue Jul 6 12:43:22 CEST 2004

Test step 1 (content.signerInfos.digestAlgorithm) -- passed

Remarks: possibility of modified content detected and signaled

End of test case TCPSD-1.11

Test case passed

Date: Tue Jul 6 12:43:22 CEST 2004

Starting test case TCPSD-1.12
Date: Tue Jul 6 12:45:10 CEST 2004
Test step 1 (content.signerInfos.signedAttrs) -- failed
Remarks: MS Outlook crashes
End of test case TCPSD-1.12
Test case failed
Date: Tue Jul 6 12:45:10 CEST 2004

Starting test case TCPSD-1.13
Date: Tue Jul 6 12:46:44 CEST 2004
Test step 1 (content.signerInfos.signedAttrs.attrType) -- passed with warning
Remarks: missleading error message, message signaled as possibly modified, processing ok
End of test case TCPSD-1.13
Test case passed with warning
Date: Tue Jul 6 12:46:44 CEST 2004

Starting test case TCPSD-1.14
Date: Tue Jul 6 12:48:09 CEST 2004
Test step 1 (content.signerInfos.signedAttrs.attr-Values) -- passed with warning
Remarks: missleading error message, message signaled as possibly modified, processing ok
End of test case TCPSD-1.14
Test case passed with warning
Date: Tue Jul 6 12:48:09 CEST 2004

Starting test case TCPSD-1.15
Date: Tue Jul 6 12:49:16 CEST 2004
Test step 1 (content.signerInfos.signatureAlgorithm) -- passed
Remarks: signatureAlgorithm ignored and retrieved elsewhere, message decoded correctly
End of test case TCPSD-1.15
Test case passed
Date: Tue Jul 6 12:49:16 CEST 2004

Starting test case TCPSD-1.16

Date: Tue Jul 6 12:50:24 CEST 2004
Test step 1 (content.signerInfos.signature) -- passed
Remarks: possible modification correctly signaled
End of test case TCPSD-1.16
Test case passed
Date: Tue Jul 6 12:50:24 CEST 2004

13.8 FC18: Processing of a Multipart/Signed S/MIME Message

Starting Test Session for: Fritz Bauspiess

Date: Tue Jul 6 14:05:27 CEST 2004

Component Under Test
Manufacturer: DATEV eG
Product Name: DATEVe:secure MAIL
Version: 1.1

Starting test case TCPSMMS-1
Date: Tue Jul 6 14:06:14 CEST 2004
Test step 1 (Content-Type) -- passed
Test step 2 (Boundary (Start of MIME entity to be signed)) -- passed
Test step 3 (Content-Type) -- passed
Test step 4 (Data to be signed) -- passed
Test step 5 (Boundary (Start of signature control information)) -- passed
Test step 6 (Content-Type) -- passed
Test step 7 (Content-Transfer-Encoding) -- passed
Test step 8 (Content-Disposition) -- passed
Test step 9 (MIME entity with signed-data) -- passed
Test step 10 (Boundary (end of multi-part/signed message)) -- passed
End of test case TCPSMMS-1
Test case passed
Date: Tue Jul 6 14:06:14 CEST 2004

Starting test case TCPSD-3

Date: Tue Jul 6 14:10:59 CEST 2004
Test step 1 (contentType) -- passed
Test step 2 (content.version) -- passed
Test step 3 (content.digest-Algorithms) -- passed with warning
Remarks: RIPEMD not supported, marked in ISIS-MTT as "+" (=SHOULD)
Test step 4 (content.encap-ContentInfo.eContentType) -- passed
Test step 5 (content.encap-ContentInfo.eContent) -- passed
Test step 6 (content.certificates) -- passed
Test step 7 (content.crls) -- passed
Test step 8 (content.signerInfos.version) -- passed
Test step 9 (content.signerInfos.sid) -- passed
Test step 10 (content.signerInfos.digestAlgorithm) -- passed with warning
Remarks: RIPEMD not supported, marked in ISIS-MTT as "+" (=SHOULD)
Test step 11 (content.signerInfos.signedAttrs) -- passed
Test step 12 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 13 (content.signerInfos.signedAttrs.attr-Values) -- passed
Test step 14 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 15 (content.signerInfos.signedAttrs.attr-Values) -- passed
Test step 16 (content.signerInfos.signedAttrs.attrType) -- passed
Test step 17 (content.signerInfos.signedAttrs.attr-Values) -- passed
Test step 18 (content.signerInfos.signatureAlgorithm) -- passed
Test step 19 (content.signerInfos.signature) -- passed
Test step 20 (content.signerInfos.unsignedAttrs) -- passed
Test step 21 (content.signerInfos.unsignedAttrs.attr-Type) -- passed
Test step 22 (content.signerInfos.unsignedAttrs.attr-Values) -- passed
End of test case TCPSD-3
Test case passed with warning
Date: Tue Jul 6 14:10:59 CEST 2004

Starting Test Session for: Fritz Bauspiess

Date: Tue Jul 6 14:11:42 CEST 2004

Component Under Test
Manufacturer: DATEV eG

Product Name: DATEVe:secure MAIL

Version: 1.1

Starting test case TCPSMMS-1.1

Date: Tue Jul 6 14:12:50 CEST 2004

Test step 1 (Content-Type) -- passed

Test step 2 (Boundary (Start of MIME entity to be signed)) -- passed

Test step 3 (Content-Type) -- passed

Test step 4 (Data to be signed) -- passed

Test step 5 (Boundary (Start of signature control information)) -- passed

Test step 6 (Content-Type) -- passed

Test step 7 (Content-Transfer-Encoding) -- passed

Test step 8 (Content-Disposition) -- passed

Test step 9 (MIME entity with invalid signed-data CMS object) -- passed

Test step 10 (Boundary (end of multipart/signed message)) -- passed

End of test case TCPSMMS-1.1

Test case passed

Date: Tue Jul 6 14:12:51 CEST 2004

Starting test case TCPSD-3.1

Date: Tue Jul 6 14:13:28 CEST 2004

Test step 1 (contentType) -- passed with warning

Remarks: missleading error message, processing ok

End of test case TCPSD-3.1

Test case passed with warning

Date: Tue Jul 6 14:13:28 CEST 2004

Starting test case TCPSD-3.2

Date: Tue Jul 6 14:14:23 CEST 2004

Test step 1 (content.version) -- passed

Remarks: illegal version ignored, message decoded correctly

End of test case TCPSD-3.2

Test case passed

Date: Tue Jul 6 14:14:23 CEST 2004

Starting test case TCPSD-3.3
Date: Tue Jul 6 14:15:17 CEST 2004
Test step 1 (content.digest-Algorithms) -- passed with warning
Remarks: missleading error message, processing ok
End of test case TCPSD-3.3
Test case passed with warning
Date: Tue Jul 6 14:15:17 CEST 2004

Starting test case TCPSD-3.4
Date: Tue Jul 6 14:16:12 CEST 2004
Test step 1 (content.encap-ContentInfo.eContentType) -- passed
Remarks: field ignored, message decoded correctly
End of test case TCPSD-3.4
Test case passed
Date: Tue Jul 6 14:16:12 CEST 2004

Starting test case TCPSD-3.5
Date: Tue Jul 6 14:17:43 CEST 2004
Test step 1 (content.encap-ContentInfo.eContent) -- passed
Remarks: possible modification correctly signaled
End of test case TCPSD-3.5
Test case passed
Date: Tue Jul 6 14:17:43 CEST 2004

Starting test case TCPSD-3.6
Date: Tue Jul 6 14:18:45 CEST 2004

Test step 1 (content.signerInfos.version) -- passed
Remarks: invalid version number ignored, message decoded correctly
End of test case TCPSD-3.6
Test case passed
Date: Tue Jul 6 14:18:45 CEST 2004

Starting test case TCPSD-3.7

Date: Tue Jul 6 14:19:42 CEST 2004
Test step 1 (content.signerInfos.sid) -- passed with warning
Remarks: missleading error message but processing ok
End of test case TCPSD-3.7
Test case passed with warning
Date: Tue Jul 6 14:19:42 CEST 2004

Starting test case TCPSD-3.8
Date: Tue Jul 6 14:21:08 CEST 2004
Test step 1 (content.signerInfos.sid) -- passed
Remarks: message correctly signaled as possibly modified
End of test case TCPSD-3.8
Test case passed
Date: Tue Jul 6 14:21:08 CEST 2004

Starting test case TCPSD-3.9
Date: Tue Jul 6 14:22:01 CEST 2004
Test step 1 (content.signerInfos.digestAlgorithm) -- passed
Remarks: message correctly signaled as possibly modified
End of test case TCPSD-3.9
Test case passed
Date: Tue Jul 6 14:22:01 CEST 2004

Starting test case TCPSD-3.10
Date: Tue Jul 6 14:22:52 CEST 2004
Test step 1 (content.signerInfos.digestAlgorithm) -- passed
Remarks: message correctly signaled as possibly modified
End of test case TCPSD-3.10
Test case passed
Date: Tue Jul 6 14:22:52 CEST 2004

Starting test case TCPSD-3.11
Date: Tue Jul 6 14:23:39 CEST 2004
Test step 1 (content.signerInfos.signedAttrs) -- failed
Remarks: MS Outlook crashes

End of test case TCPSD-3.11

Test case failed

Date: Tue Jul 6 14:23:39 CEST 2004

Starting test case TCPSD-3.12

Date: Tue Jul 6 14:25:30 CEST 2004

Test step 1 (content.signerInfos.signedAttrs.attrValues) -- passed

Remarks: different content of content.signerInfos.signedAttrs.attrValues ignored, message decoded correctly

End of test case TCPSD-3.12

Test case passed

Date: Tue Jul 6 14:25:30 CEST 2004

Starting test case TCPSD-3.13

Date: Tue Jul 6 14:26:23 CEST 2004

Test step 1 (content.signerInfos.signedAttrs) -- passed with warning

Remarks: missleading error message but processing ok

End of test case TCPSD-3.13

Test case passed with warning

Date: Tue Jul 6 14:26:23 CEST 2004

Starting test case TCPSD-3.14

Date: Tue Jul 6 14:27:28 CEST 2004

Test step 1 (content.signerInfos.signedAttrs) -- passed with warning

Remarks: missleading error message but processing ok

End of test case TCPSD-3.14

Test case passed with warning

Date: Tue Jul 6 14:27:28 CEST 2004

Starting test case TCPSD-3.15

Date: Tue Jul 6 14:29:31 CEST 2004

Test step 1 (content.signerInfos.signedAttrs.attrValues) -- passed

Remarks: invalid value ignored, message decoded correctly

End of test case TCPSD-3.15

Test case passed

Date: Tue Jul 6 14:29:31 CEST 2004

Starting test case TCPSD-3.16
Date: Tue Jul 6 14:30:33 CEST 2004
Test step 1 (content.signerInfos.signedAttrs) -- passed with warning
Remarks: missleading error message but processing ok
End of test case TCPSD-3.16
Test case passed with warning
Date: Tue Jul 6 14:30:33 CEST 2004

Starting test case TCPSD-3.17
Date: Tue Jul 6 14:31:20 CEST 2004
Test step 1 (content.signerInfos.signedAttrs.attrValues) -- passed with warning
Remarks: missleading error message but processing ok
End of test case TCPSD-3.17
Test case passed with warning
Date: Tue Jul 6 14:31:20 CEST 2004

Starting test case TCPSD-3.18
Date: Tue Jul 6 14:32:59 CEST 2004
Test step 1 (content.signerInfos.signatureAlgorithm) -- passed
Remarks: signature algorithm ignored and retrieved elsewhere, message decoded correctly
End of test case TCPSD-3.18
Test case passed
Date: Tue Jul 6 14:32:59 CEST 2004

Starting test case TCPSD-3.19
Date: Tue Jul 6 14:33:50 CEST 2004
Test step 1 (content.signerInfos.signature) -- passed
Remarks: message correctly signaled as possibly modified
End of test case TCPSD-3.19
Test case passed
Date: Tue Jul 6 14:33:50 CEST 2004

13.9 FC29: Processing of a valid, 3-step certificate path

Starting Test Session for: Fritz Bauspiess

Date: Tue Jul 6 13:44:53 CEST 2004

Component Under Test
Manufacturer: DATEV eG
Product Name: DATEVe:secure MAIL
Version: 1.1

Starting test case TCPVVALID-1
Date: Tue Jul 6 13:48:54 CEST 2004

Test step 1 (BuildAndValidateCertPath()) -- passed
End of test case TCPVVALID-1
Test case passed
Date: Tue Jul 6 13:48:54 CEST 2004

13.10 FC30: Processing of an invalid certificate path

Starting Test Session for: Fritz Bauspiess

Date: Tue Jul 6 13:49:47 CEST 2004

Component Under Test
Manufacturer: DATEV eG
Product Name: DATEVe:secure MAIL
Version: 1.1

Starting test case TCPVSIGINVALID-1
Date: Tue Jul 6 13:52:17 CEST 2004
Test step 1 (ValidateCertPath()) -- passed
Test step 2 (BuildAndValidateCertPath()) -- passed
End of test case TCPVSIGINVALID-1
Test case passed
Date: Tue Jul 6 13:52:17 CEST 2004

Starting test case TCPVSIGINVALID-2
Date: Tue Jul 6 13:54:09 CEST 2004
Test step 1 (ValidateCertPath()) -- passed
Test step 2 (BuildAndValidateCertPath()) -- passed
End of test case TCPVSIGINVALID-2
Test case passed
Date: Tue Jul 6 13:54:09 CEST 2004

Starting test case TCPVCERTREVO-1
Date: Tue Jul 6 13:56:07 CEST 2004
Test step 1 (CheckStatusUsingCRL()) -- passed
Test step 2 (CheckRevocationStatus()) -- passed
Test step 3 (ValidateCertPath()) -- passed
Test step 4 (BuildAndValidateCertPath()) -- passed
End of test case TCPVCERTREVO-1
Test case passed
Date: Tue Jul 6 13:56:07 CEST 2004

Starting test case TCPVEXPIRED-1
Date: Tue Jul 6 13:56:46 CEST 2004
Test step 1 (ValidateCertPath()) -- passed
Test step 2 (BuildAndValidateCertPath()) -- passed
End of test case TCPVEXPIRED-1
Test case passed
Date: Tue Jul 6 13:56:46 CEST 2004

Starting test case TCPVINVALIDCA-1
Date: Tue Jul 6 14:00:51 CEST 2004
Test step 1 (ValidateCertPath()) -- passed
Test step 2 (BuildAndValidateCertPath()) -- passed
End of test case TCPVINVALIDCA-1
Test case passed
Date: Tue Jul 6 14:00:51 CEST 2004