



# TC TrustCenter

  

## TC Enterprise ID Certificate Profiles

---

TC Enterprise ID  
Version 1.8

Hamburg, Germany  
April 2011

---

**Geschäftsführung**  
Austin McCabe  
Kristen Laubscher

**HRB 96168 AG Hamburg**  
**Ust.-ID-Nr. DE245979558**

**Bankverbindung**  
Bank of America  
BLZ 50010900  
Kto.-Nr. 9160016  
**IBAN DE14 5001 0900 0019 1600 16**  
**BIC BOFADE33**

Sonninstraße 24-28  
20097 Hamburg, Germany

Postfach 10 60 49  
20041 Hamburg, Germany

Phone: +49 (0)40 / 80 80 26-0

Fax: +49 (0)40 / 80 80 26-1 26

<http://www.trustcenter.de>

---

Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung von TC TrustCenter unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Verbreitungen, Übersetzungen oder die Verwendung in elektronischen Systemen. Ausgenommen hiervon sind das Kopieren und der Ausdruck zum eigenen Gebrauch.

Alle Informationen in diesem Dokument wurden mit größter Sorgfalt erstellt. Weder TC TrustCenter noch der Autor können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Dokumentes stehen.

„TC TrustCenter“, das TC TrustCenter-Logo, „Ident Point“, „TC PKI“ und „TC Info Line“ sind eingetragene Marken der TC TrustCenter GmbH.

Alle in diesem Dokument verwendeten, aber hier nicht genannten Marken- oder Produktnamen sind Marken oder Warenzeichen der entsprechenden Inhaber.

Copyright © 2009 TC TrustCenter GmbH

Alle Rechte vorbehalten.

---

All rights reserved. No information or images, fully or partially, in any form or by any means, may be reproduced, copied, duplicated, published or used in electronic systems or translations without the prior written consent of TC TrustCenter. This represents a crime, excluding printing and duplicating for one's own use.

All information in this document is compiled with great care. Neither TC TrustCenter nor the author are liable for any damages or disservice, that are in connection with the use of this document.

„TC TrustCenter“, the TC TrustCenter logo, „Ident Point“, „TC PKI“ and „TC Info Line“ are registered trademarks of the TC TrustCenter GmbH.

All brands, product names and trademarks used in this document, but not listed above, are trademarks or service marks of the respective owners.

Copyright © 2009 TC TrustCenter GmbH



## Table of Contents

1	Certificate Profiles .....	5
1.1	“TC Business ID Demo, 30 days” .....	6
1.2	“SCEP TC Business ID Demo, 30 days” .....	8
1.3	“TC Business ID Demo, recoverable, 30 days” .....	10
1.4	“SCEP VPN ID Demo, 30 days” .....	12
1.5	“TC Client Computer ID Demo, 30 days” .....	14
1.6	“SCEP TC Client Computer ID Demo, 30 days” .....	16
1.7	“TC Business ID for Adobe Demo .....	18
1.8	“TC Trust SSL Demo, 30 days” .....	20
1.9	“TC Personal ID, 1yr”; 2 yrs or 3 yrs .....	22
1.10	“TC Business ID, 1yr”; 2 yrs or 3 yrs .....	24
1.11	“SCEP TC Business ID, 1yr”; 2 yrs or 3 yrs .....	26
1.12	“TC Business ID, recoverable, 1yr”; 2 yrs or 3 yrs .....	28
1.13	“TC Business ID, sign+auth, 1yr”; 2 yrs or 3 yrs .....	30
1.14	“TC Business ID, sign, 1yr”; 2 yrs or 3 yrs .....	32
1.15	“TC Business ID, auth, 1yr”; 2 yrs or 3 yrs .....	34
1.16	“TC Business ID, recoverable enc, 1yr”; 2 yrs or 3 yrs .....	36
1.17	“TC Business ID for Adobe, 1yr”; 2 yrs or 3 yrs .....	38
1.18	“TC Enrollment Agent ID, 1yr”; 2 yrs or 3 yrs .....	40
1.19	“TC Domain Controller ID, 1yr”; 2 yrs or 3 yrs .....	42
1.20	“TC RAS and IAS Server ID, 1yr”; 2 yrs or 3 yrs .....	44
1.21	“SCEP TC VPN ID, 1yr”; 2 yrs or 3 yrs .....	46
1.22	“TC Client Computer ID, 1yr”; 2 yrs or 3 yrs .....	48
1.23	“SCEP TC Client Computer ID, 1yr”; 2 yrs or 3 yrs .....	50
1.24	“TC Team Certificate, 1yr”; 2yrs or 3yrs .....	52
1.25	“TC Gateway Certificate, 1yr”; 2yrs or 3yrs .....	54
1.26	“TC Publisher ID for Adobe AIR, 1yr”; 2yrs or 3yrs .....	56
1.27	“TC Publisher ID for Microsoft Authenticode, 1yr”; 2yrs or 3yrs .....	58
1.28	“TC Publisher ID for Java Desktop, 1yr”; 2yrs or 3yrs .....	60



## 1 Certificate Profiles

This document describes the certificate hierarchy and the profile of the certificates.

Please note that in the following sections the following fields are always written to refer to the “XI” Sub-CA certificate:

- Issuer
- AuthorityInfoAccess caIssuers URL
- AuthorityInfoAccess OCSP URL
- CRLDistributionPoint

The “XI” has to be replaced by the appropriate roman number depending on the Sub-CA certificate being used.

**Note:** Not all certificate profiles and not all certificate validity periods are supported by AutoEnrollment or by API enrollment. Please refer to the statement of service document for the list of certificate templates available for AutoEnrollment.

**Note:** Only certificate profiles starting with *SCEP* are suited for enrollment using the *SCEP* interface.

## 1.1 “TC Business ID Demo, 30 days”

This certificate profile is to be used for demonstration purposes only. The certificates are chained to the TC Class 1 CA.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 1 L1 CA IX	DirectoryName
	OU	TC TrustCenter Class 1 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 30 days		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.1 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt">http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de">http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl">http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.13.1.1 Version=<according to current configuration, e.g. 100.1>



## 1.2 “SCEP TC Business ID Demo, 30 days”

This certificate profile is to be used for demonstration purposes only. The certificates are chained to the TC Class 1 CA. All certificate profiles beginning with SCEP are intended for SCEP enrollment only.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 1 L1 CA IX	DirectoryName
	OU	TC TrustCenter Class 1 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 30 days		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.1 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt">http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de">http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl">http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl</a>

### 1.3 “TC Business ID Demo, recoverable, 30 days”

This certificate profile is to be used for demonstration purposes only. The certificates are chained to the TC Class 1 CA.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 1 L1 CA IX	DirectoryName
	OU	TC TrustCenter Class 1 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 30 days		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	2048 bit RSA		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.1 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt">http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de">http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl">http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.13.2.1 Version=<according to current configuration, e.g. 100.1>

## 1.4 “SCEP VPN ID Demo, 30 days”

This certificate profile is to be used for demonstration purposes only. The certificates are chained to the TC Class 0 Root. This root certificate is not pre-installed in popular web browsers and can be downloaded from the TC TrustCenter [homepage](#). All certificate profiles beginning with *SCEP* are intended for *SCEP* enrollment only.

Data Field	Value		
Version	v3		
Serial Number	[Automatic number according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption		
Issuer	Attribute	Value	Encoding
	Email	certificate@trustcenter.de	IA5String
	OU	TC TrustCenter Class 0 CA	DirectoryName
	O	TC TrustCenter AG	DirectoryName
	L	Hamburg	DirectoryName
	SP	Hamburg	DirectoryName
	C	DE	PrintableString
Validity	[Date of Issuance] + 30 days		
Subject	Attribute	Value	Encoding
	CN	<FQDN of network device as specified in the request>	DirectoryName
	OU	<as specified in request>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
	DC	<as specified in request>	IA5String
Subject Public Key	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature keyEncipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.1 (Server Authentication) 1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.8.2.2 (iKEIntermediate)
<b>netscapeCertificate Type</b>	no	SSL-Client Authentication SSL-Server-Authentication
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.0 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tcclass0.crt">http://www.trustcenter.de/certservices/cacerts/tcclass0.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.tcclass0.trustcenter.de">http://ocsp.tcclass0.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://www.trustcenter.de/crl/v2/tcclass0.crl">http://www.trustcenter.de/crl/v2/tcclass0.crl</a>

## 1.5 “TC Client Computer ID Demo, 30 days”

This certificate profile is to be used for demonstration purposes only. The certificates are chained to the TC Class 1 CA.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 1 L1 CA IX	DirectoryName
	OU	TC TrustCenter Class 1 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 30 days		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	Name of client computer	DirectoryName
	OU	<as specified in request>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
	DC	<as specified in request>	IA5String
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	Digital Signature, Key Encipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.2 (Client Authentication)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.1 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	DNS-Name=<FQDN as specified in request>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: <a href="http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt">URL=http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt</a> accessMethod: ocsp accessLocation: <a href="http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de">URL=http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl">http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.18.1.0 Version=<according to current configuration, e.g. 100.1>

## 1.6 “SCEP TC Client Computer ID Demo, 30 days”

This certificate profile is to be used for demonstration purposes only. The certificates are chained to the TC Class 1 CA. All certificate profiles beginning with SCEP are intended for SCEP enrollment only.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 1 L1 CA IX	DirectoryName
	OU	TC TrustCenter Class 1 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 30 days		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	Name of client computer	DirectoryName
	OU	<as specified in request>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
	DC	<as specified in request>	IA5String
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	Digital Signature, Key Encipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.2 (Client Authentication)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.1 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	DNS-Name=<FQDN as specified in request>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: <a href="http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt">URL=http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt</a> accessMethod: ocsp accessLocation: <a href="http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de">URL=http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl">http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl</a>

## 1.7 “TC Business ID for Adobe Demo

This certificate profile is to be used for demonstration purposes only. The certificates are chained to the CDS Root. A flag in the certificate causes a warning message box to appear whenever a PDF signed with this certificate is being opened.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter CA for Adobe I	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 30 days		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TEST	PrintableString
	OU	<according to Organization Unit of the User>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	2048 bit RSA		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	Non-repudiation, digital signature
<b>extKeyUsage</b>	no	PDF Signature (1.2.840.113583.1.1.5)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.840.113583.1.2.2 cPSuri = <a href="http://www.trustcenter.de/cps">http://www.trustcenter.de/cps</a>
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: ocsf accessLocation: URL= <a href="http://ocsp.l.adobe-cds.trustcenter.de">http://ocsp.l.adobe-cds.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://www.trustcenter.de/crl/v2/tc_ca_for_adobe_l.crl">http://www.trustcenter.de/crl/v2/tc_ca_for_adobe_l.crl</a>
<b>Archive Revocation Info</b>	no	True
<b>TimeStamp URL</b>	no	<a href="http://tss.l.adobe-cds.trustcenter.de">tss.l.adobe-cds.trustcenter.de</a>

## 1.8 “TC Trust SSL Demo, 30 days”

This certificate profile is to be used for demonstration purposes only. The certificates are chained to the TC Class 0 Root. This root certificate is not pre-installed in popular web browsers and can be downloaded from the TC TrustCenter [homepage](#).

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	Email	certificate@trustcenter.de	IA5String
	OU	TC TrustCenter Class 0 CA	DirectoryName
	O	TC TrustCenter AG	DirectoryName
	L	Hamburg	DirectoryName
	SP	Hamburg	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 30 days		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<FQDN of the SSL server as specified in request>	DirectoryName
	OU	<as specified in request>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.1 (Server Authentication) 1.3.6.1.5.5.7.3.2 (Client Authentication)
<b>netscapeCertificateType</b>	no	SSL-Client Authentication SSL-Server-Authentication
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.0 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tcclass0.crt">http://www.trustcenter.de/certservices/cacerts/tcclass0.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.tcclass0.trustcenter.de">http://ocsp.tcclass0.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://www.trustcenter.de/crl/v2/tcclass0.crl">http://www.trustcenter.de/crl/v2/tcclass0.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.16.1 Version=<according to current configuration, e.g. 100.1>

### 1.9 “TC Personal ID, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for real applications. The certificates are chained to the TC Class 1 CA. The certificate will have no Organization-field in the subject-DN, they are intended for external partners or contractors.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 1 L1 CA IX	DirectoryName
	OU	TC TrustCenter Class 1 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.1 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt">http://www.trustcenter.de/certservices/cacerts/tc_class1_L1_CA_IX.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de">http://ocsp.IX.tcclass1.tcuniversal-i.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl">http://crl.IX.tcclass1.tcuniversal-i.trustcenter.de/crl/v2/tc_class1_L1_CA_IX.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.12.1.1 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.10 “TC Business ID, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for real applications. It is not recoverable. The certificates are chained to the TC Class 2 Root.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.13.3.1 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>



### 1.11 “SCEP TC Business ID, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for real applications. It is not recoverable. The certificates are chained to the TC Class 2 Root. All certificate profiles beginning with *SCEP* are intended for *SCEP* enrollment only.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>

### 1.12 “TC Business ID, recoverable, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for real applications. The certificates are chained to the TC Class 2 Root.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	2048 bit RSA		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.13.4.1 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.13 “TC Business ID, sign+auth, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for signature and authentication applications. The certificates are chained to the TC Class 2 Root.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplateInformation</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.13.3.2 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.14 “TC Business ID, sign, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for signature applications. The certificates are chained to the TC Class 2 Root.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	O	<according to Organization of the affiliate associated with the requesting user >	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation
<b>extKeyUsage</b>	no	emailProtection (1.3.6.1.5.5.7.3.4)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.13.3.4 append “.2” or “.3” in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.15 “TC Business ID, auth, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for authentication applications. The certificates are chained to the TC Class 2 Root.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplateInformation</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.13.3.5 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.16 “TC Business ID, recoverable enc, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for encryption and decryption applications, e.g. email encryption. The certificates are chained to the TC Class 2 Root.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	2048 bit RSA		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	keyEncipherment, dataEncipherment
<b>extKeyUsage</b>	no	emailProtection (1.3.6.1.5.5.7.3.4) Encrypting File System (1.3.6.1.4.1.311.10.3.4)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplateInformation</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.13.4.3 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.17 “TC Business ID for Adobe, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for PDF signature only. The certificates are chained to the CDS Root.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter CA for Adobe I	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	2048 bit RSA		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	Non-repudiation, digital signature
<b>extKeyUsage</b>	no	PDF Signature (1.2.840.113583.1.1.5)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.840.113583.1.2.1 cPSuri = <a href="http://www.trustcenter.de/cps">http://www.trustcenter.de/cps</a>
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: ocsf accessLocation: URL= <a href="http://ocsp.l.adobe-cds.trustcenter.de">http://ocsp.l.adobe-cds.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://www.trustcenter.de/crl/v2/tc_ca_for_adobe_l.crl">http://www.trustcenter.de/crl/v2/tc_ca_for_adobe_l.crl</a>
<b>Archive Revocation Info</b>	no	True
<b>TimeStamp URL</b>	no	<a href="http://tss.l.adobe-cds.trustcenter.de">tss.l.adobe-cds.trustcenter.de</a>

### 1.18 “TC Enrollment Agent ID, 1yr”; 2 yrs or 3 yrs

This certificate profile is to be used for enrollment agents. The certificates are chained to the TC Class 2 Root.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<according to GivenName + Surname of the User>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	Serial-Number	<according to External ID of the User>	PrintableString
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) MS SmartCardLogon (1.3.6.1.4.1.311.20.2.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7) Certificate Request Agent (1.3.6.1.4.1.311.20.2.1)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	Other Name / UPN (1.3.6.1.4.1.311.20.2.3) = <Windows User Login Name (User Principal Name)> rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplateInformation</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.14.1.1 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.19 “TC Domain Controller ID, 1yr”; 2 yrs or 3 yrs

In order to setup smart card logon the domain controller must be equipped with this type of certificate.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	Name of domain controller	DirectoryName
	OU	<as specified>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
	DC	<as specified in request>	IA5String
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	Digital Signature, Key Encipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.1 (Server Authentication) 1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.4.1.311.20.2.2 (Smart Card Logon)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	DNS-Name=<FQDN as specified in request> RFC822-Name=<as specified in request> GUID[1.3.6.1.4.1.311.25.1] = <as specified in request>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplate-Information</b>	no	TemplateName (1.3.6.1.4.1.311.20.2) = „DomainController“ (BMPString)
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.17.1 append “.2” or “.3” in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

## 1.20 “TC RAS and IAS Server ID, 1yr”; 2 yrs or 3 yrs

This certificate is intended for IAS and RAS servers.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	Name of RAS and IAS server	DirectoryName
	OU	<as specified>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
	DC	<as specified in request>	IA5String
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	Digital Signature, Key Encipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.1 (Server Authentication) 1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.8.2.2 (iKEIntermediate)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	DNS-Name=<FQDN as specified in request>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplateInformation</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.17.2 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.21 “SCEP TC VPN ID, 1yr”; 2 yrs or 3 yrs

This certificate is intended for network devices. All certificate profiles beginning with *SCEP* are intended for *SCEP* enrollment only.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<FQDN of network device as specified in the request>	DirectoryName
	OU	<as specified>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
	DC	<as specified in request>	IA5String
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature keyEncipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.1 (Server Authentication) 1.3.6.1.5.5.7.3.2 (Client Authentication) 1.3.6.1.5.5.8.2.2 (iKEIntermediate)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	DNS-Name=<FQDN as specified in request>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>

## 1.22 “TC Client Computer ID, 1yr”; 2 yrs or 3 yrs

This certificate is intended to be used for machine authentication.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	Name of client computer	DirectoryName
	OU	<as specified in request>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	Digital Signature, Key Encipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.2 (Client Authentication)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	DNS-Name=<FQDN as specified in request>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplateInformation</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.18.1 append “.2” or “.3” in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.23 “SCEP TC Client Computer ID, 1yr”; 2 yrs or 3 yrs

This certificate is intended to be used for machine authentication. All certificate profiles beginning with *SCEP* are intended for *SCEP* enrollment only.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	Name of client computer	DirectoryName
	OU	<as specified in request>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
	DC	<as specified in request>	IA5String
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	Digital Signature, Key Encipherment
<b>extKeyUsage</b>	no	1.3.6.1.5.5.7.3.2 (Client Authentication)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	DNS-Name=<FQDN as specified in request>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>

### 1.24 “TC Team Certificate, 1yr”; 2yrs or 3yrs

Team certificates are intended to be shared among several members of a team as opposed to be exclusively used by the “Certificate Owner” like the TC Business ID.

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<Team name according to request> + “Team Certificate”	DirectoryName
	OU	<as specified in request>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) IPsec User (1.3.6.1.5.5.7.3.7)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: calssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= 1.2.276.0.44.5.1.15.1.1 append ".2" or ".3" in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

### 1.25 “TC Gateway Certificate, 1yr”; 2yrs or 3yrs

Gateway certificates are intended to be used by E-Mail gateways or the Microsoft System Center Configuration Manager. The following function names are approved:

- "Secure Mail Gateway"
- "E-mail Gateway"
- "Automatic Mail Signature " or "Automatische Mail Signatur"
- "Mail Encryption" or "Mailverschlüsselung"
- "Archive Services" or "Archivservice"
- "The site code of this site server is <XXX>"

Data Field	Value		
<b>Version</b>	v3		
<b>Serial Number</b>	[Automatic number according to TC TrustCenter standard]		
<b>Signature Algorithm</b>	sha1withRSAEncryption		
<b>Issuer</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	TC TrustCenter Class 2 L1 CA XI	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
<b>Validity</b>	[Date of Issuance] + 1, 2 or 3 years		
<b>Subject</b>	<b>Attribute</b>	<b>Value</b>	<b>Encoding</b>
	CN	<approved function name as specified in the request>	DirectoryName
	OU	<as specified in request>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
<b>Subject Public Key</b>	<according to certificate request>		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature keyEncipherment dataEncipherment
<b>extKeyUsage</b>	no	emailProtection (1.3.6.1.5.5.7.3.4) documentSigning (1.3.6.1.4.1.311.10.3.12)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a>
<b>subjectAltNames</b>	no	rfc822-Name = <Email Address>
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XI.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XI.tcclass2-ii.trustcenter.de">http://ocsp.XI.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl">http://crl.XI.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XI.crl</a>
<b>certificateTemplate-Information</b>	no	Extension is only present if AutoEnrollment has been used to request the certificate. Template OID= TBD append “.2” or “.3” in case of 2 or 3 years validity Version=<according to current configuration, e.g. 100.1>

## 1.26 “TC Publisher ID for Adobe AIR, 1yr”; 2yrs or 3yrs

Certificate for signing Adobe AIR code.

Data Field	Value		
Version	v3		
Serial Number	[Automatic number according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption		
Issuer	Attribute	Value	Encoding
	CN	TC TrustCenter Class 2 L1 CA XII	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
Validity	[Date of Issuance] + 1, 2 or 3 years		
Subject	Attribute	Value	Encoding
	CN	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	OU	TC Publisher ID for <application name, e.g. Adobe AIR>	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
Subject Public Key	<according to certificate request>, at least 2048 bit RSA key length!		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature
<b>extKeyUsage</b>	no	codeSigning (1.3.6.1.5.5.7.3.3)
<b>nsCertType</b>	no	Code-Signatur (10)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a> [2] Policy-OID 1.2.276.0.44.1.1.1.2.2.3.1
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XII.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XII.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XII.tcclass2-ii.trustcenter.de">http://ocsp.XII.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XII.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XII.crl">http://crl.XII.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XII.crl</a>

### 1.27 “TC Publisher ID for Microsoft Authenticode, 1yr”; 2yrs or 3yrs

Certificate for Microsoft Authenticode.

Data Field	Value		
Version	v3		
Serial Number	[Automatic number according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption		
Issuer	Attribute	Value	Encoding
	CN	TC TrustCenter Class 2 L1 CA XII	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
Validity	[Date of Issuance] + 1, 2 or 3 years		
Subject	Attribute	Value	Encoding
	CN	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	OU	TC Publisher ID for Authenticode	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
Subject Public Key	<according to certificate request>, at least 2048 bit RSA key length		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation
<b>extKeyUsage</b>	no	codeSigning (1.3.6.1.5.5.7.3.3) Kernel Mode Code Signing (1.3.6.1.4.1.311.61.1.1)
<b>nsCertType</b>	no	Code-Signatur (10)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a> [2] Policy-OID 1.2.276.0.44.1.1.1.2.2.1.1
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XII.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XII.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XII.tcclass2-ii.trustcenter.de">http://ocsp.XII.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XII.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XII.crl">http://crl.XII.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XII.crl</a>

### 1.28 “TC Publisher ID for Java Desktop, 1yr”; 2yrs or 3yrs

Certificate for signing Java code for desktop applications.

Data Field	Value		
Version	v3		
Serial Number	[Automatic number according to TC TrustCenter standard]		
Signature Algorithm	sha1withRSAEncryption		
Issuer	Attribute	Value	Encoding
	CN	TC TrustCenter Class 2 L1 CA XII	DirectoryName
	OU	TC TrustCenter Class 2 L1 CA	DirectoryName
	O	TC TrustCenter GmbH	DirectoryName
	C	DE	PrintableString
Validity	[Date of Issuance] + 1, 2 or 3 years		
Subject	Attribute	Value	Encoding
	CN	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	OU	<according to Organization Unit of the User>	DirectoryName
	OU	TC Publisher ID for Java Desktop	DirectoryName
	O	<according to Organization of the affiliate associated with the requesting user>	DirectoryName
	L	<according to Location of the affiliate associated with the requesting user>	DirectoryName
	SP	<according to State of the affiliate associated with the requesting user>	DirectoryName
	C	<according to Country of the affiliate associated with the requesting user>	PrintableString
Subject Public Key	<according to certificate request>, at least 2048 bit RSA key length		

Extension	Crit.	Value
<b>basicConstraints</b>	yes	cA: FALSE
<b>keyUsage</b>	yes	digitalSignature nonRepudiation
<b>extKeyUsage</b>	no	codeSigning (1.3.6.1.5.5.7.3.3)
<b>nsCertType</b>	no	Code-Signatur (10)
<b>certificatePolicies</b>	no	[1] Policy-OID 1.2.276.0.44.1.1.1.2 cPSuri = <a href="http://www.trustcenter.de/guidelines">http://www.trustcenter.de/guidelines</a> [2] Policy-OID 1.2.276.0.44.1.1.1.2.2.2.1
<b>subjectKeyIdentifier</b>	no	[Key-ID of this Certificate]
<b>authorityKeyIdentifier</b>	no	[Key-ID of Issuer Certificate]
<b>authorityInfoAccess</b>	no	accessMethod: caIssuers accessLocation: URL= <a href="http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XII.crt">http://www.trustcenter.de/certservices/cacerts/tc_class2_L1_CA_XII.crt</a> accessMethod: ocsp accessLocation: URL= <a href="http://ocsp.XII.tcclass2-ii.trustcenter.de">http://ocsp.XII.tcclass2-ii.trustcenter.de</a>
<b>cRLDistributionPoints</b>	no	<a href="http://crl.XII.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XII.crl">http://crl.XII.tcclass2-ii.trustcenter.de/crl/v2/tc_class2_L1_CA_XII.crl</a>