

# Digital Tachograph DTCO 1381 Security Target

**Author:** Winfried Rogenz | CVAM TTS LRH

**Revision:** 1.17


**Maturity:** <initial / final>

**Status:** <draft / **released** / obsolete>

**Release:** DTCO 1381, Release 2.2

**File:** 1381R2..0276.Security\_Target.doc

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				1 of 106	
		Document key					
Villingen-Schwenningen (VL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

## 1 History

Rev.	Date	Maturity	Author	Reason
1.0	03.04.2009	final	Winfried Rogenz	Changing of TOE reference, adoption from document 1382._SEC.01.Security_Target.doc, version 1.11, 09.12.2008
1.1	29.04.2009	final	Winfried Rogenz	Correction table page 63
1.2	17.02.2011	Final	Winfried Rogenz	Amendment after publishing protection profile BSI-CC-PP-057
1.3	05.09.2011	Final	Winfried Rogenz	Correction after remarks from the evaluator
1.4	20.09.2011	Final	Winfried Rogenz	Correction after remarks from the evaluator
1.5	06.10.2011	Final	Winfried Rogenz	Formal Corrections
1.6	25.04.2012	Final	Winfried Rogenz	Formal corrections after TOE-Design
1.7	09.05.2012	Final	Winfried Rogenz	Correction after remarks from the certification body
1.8	09.05.2012	Final	Winfried Rogenz	Fornal Corrections
1.9	10.05.2012	Final	Winfried Rogenz	Figure 1 corrected
1.10	26.07.2012	final	Winfried Rogenz	Update for Release 2.1
1.11	15.10.2012	final	Winfried Rogenz	Formal Corrections
1.12	15.11.2012	Final	Winfried Rogenz	Typographic and formal corrections
1.13	16.01.2014	Final	Winfried Rogenz	Update for Release 2.2
1.14	28.07.2014	final	Winfried Rogenz	Change Request for Release 2.2
1.15	02.09.2014	final	Winfried Rogenz	Update Change Request for Release 2.2
1.16	04.09.2014	final	Winfried Rogenz	Formal and typographic corrections
1.17	11.02.2015 final		Winfried Rogenz	Chapter 3.2, 4.3.4 corrected


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						2 of 106	
Villingen-Schwenningen (VL)		Copyright ( C ) Continental AG 2008					

## 2 Table of Contents

<b>1</b>	<b>History .....</b>	<b>2</b>
<b>2</b>	<b>Table of Contents .....</b>	<b>3</b>
<b>3</b>	<b>Terms and Abbreviations.....</b>	<b>6</b>
3.1	Terms .....	6
3.2	Abbreviations.....	11
<b>4</b>	<b>ST Introduction .....</b>	<b>13</b>
4.1	ST reference.....	13
4.2	TOE reference .....	13
4.3	TOE overview .....	13
4.3.1	TOE definition and operational usage .....	13
4.3.2	TOE major security features for operational use .....	15
4.3.3	TOE Type.....	16
4.3.4	Non-TOE hardware/software/firmware.....	17
<b>5</b>	<b>Conformance claims .....</b>	<b>18</b>
5.1	CC conformance claim .....	18
5.2	PP conformance claim.....	18
5.3	Package claim .....	18
<b>6</b>	<b>Security problem definition .....</b>	<b>20</b>
6.1	Introduction.....	20
6.2	Threats .....	23
6.2.1	Threats averted solely by the TOE.....	23
6.2.2	Threats averted by the TOE and its operational environment .....	24
6.2.3	Threats averted solely by the TOE's operational environment.....	25
6.3	Organisational security policies .....	25
6.3.1	OSPs related to the TOE .....	25
6.3.2	OSPs related to the TOE and its operational environment.....	25
6.3.3	OSPs related to the TOE's operational environment.....	26


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 3 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

6.4	Assumptions .....	27
<b>7</b>	<b>Security objectives .....</b>	<b>28</b>
7.1	Security objectives for the TOE .....	28
7.2	Security objectives for the operational environment .....	29
7.2.1	Design environment (cf. the life cycle diagram in Figure 2 above) .....	29
7.2.2	Manufacturing environment.....	29
7.2.3	Fitter and workshops environment .....	30
7.2.4	End user environment .....	30
7.3	Security objectives rationale .....	32
<b>8</b>	<b>Extended components definition .....</b>	<b>40</b>
8.1	Extended components definition.....	40
<b>9</b>	<b>Security requirements.....</b>	<b>41</b>
9.1	Security functional requirements .....	41
9.1.1	Overview .....	42
9.1.2	Class FAU Security Audit.....	46
9.1.2.1	FAU_GEN - Security audit data generation.....	46
9.1.2.2	FAU_SAR - Security audit review.....	47
9.1.2.3	FAU_STG - Security audit event storage .....	47
9.1.3	Class FCO Communication.....	48
9.1.3.1	FCO_NRO Non-repudation of origin .....	48
9.1.4	Class FCS Cryptographic Support .....	48
9.1.4.1	FCS_CKM - Cryptographic key management .....	48
9.1.4.2	FCS_COP Cryptographic operation .....	53
9.1.5	Class FDP User Data Protection.....	53
9.1.5.3	FDP_ACC Access control policy .....	53
9.1.5.4	FDP_ACF - Access control functions .....	55
9.1.5.5	FDP_ETC Export from the TOE .....	57
9.1.5.6	FDP_ITC Import from outside of the TOE .....	58
9.1.5.7	FDP_RIP Residual information protection.....	59
9.1.5.8	FDP_SDI Stored data integrity .....	60
9.1.6	Class FIA Identification and Authentication.....	60


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						4 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

9.1.6.1	FIA_AFL Authentication failures .....	60
9.1.6.2	FIA_ATD User attribute definition .....	61
9.1.7	FIA_UAU User authentication .....	62
9.1.7.3	FIA_UID - User identification .....	64
9.1.8	Class FMT Security Management .....	65
9.1.8.1	FMT_MSA - Management of security attributes .....	65
9.1.8.2	FMT_MOF - Management of functions in TSF .....	66
9.1.8.3	Specification of Management Functions (FMT_SMF) .....	67
9.1.9	Class FPR Privacy (FPR) .....	67
9.1.9.1	FPR_UNO - Unobservability .....	67
9.1.10	Protection of the TSF (FPT) .....	67
9.1.10.2	FPT_FLS - Fail secure .....	67
9.1.10.3	FPT_PHP - TSF physical protection .....	68
9.1.10.4	FPT_STM - Time stamps .....	68
9.1.10.5	FPT_TDC – Inter-TSF TSF Data Consistency .....	69
9.1.10.6	FPT_TST - TSF self test .....	69
9.1.11	Resource Utilisation (FRU) .....	70
9.1.11.7	FRU_PRS - Priority of service .....	70
9.2	Security assurance requirements .....	70
9.3	Security requirements rationale .....	72
9.3.1	Security functional requirements rationale .....	72
9.3.2	Rationale for SFR's Dependencies .....	87
9.3.3	Security Assurance Requirements Rationale .....	87
9.3.4	Security Requirements – Internal Consistency .....	88
<b>10</b>	<b>TOE summary specification .....</b>	<b>90</b>
<b>11</b>	<b>Reference documents .....</b>	<b>96</b>
<b>12</b>	<b>Annex A .....</b>	<b>98</b>

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 5 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

## 3 Terms and Abbreviations

### 3.1 Terms

Term	Explanation
<b>Activity data</b>	Activity data include user activities data, events and faults data and control activity data. Activity data are part of User Data.
<b>Application note</b>	Optional informative part of the ST containing sensible supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
<b>Approved Workshops</b>	Fitters and workshops installing, calibrating and (optionally) repairing VU and being under such agreement with a VU manufacturer, so that the assumption A.Approved_Workshops is fulfilled.
<b>Authenticity</b>	Ability to confirm that an entity itself and the data elements stored in were issued by the entity issuer
<b>Certificate chain</b>	Hierarchical sequence of Equipment Certificate (lowest level), Member State Certificate and European Public Key (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level
<b>Certification authority</b>	A natural or legal person who certifies the assignment of public keys (for example PK.EQT) to serial number of equipment and to this end holds the licence
<b>Digital Signature</b>	A digital signature is a seal affixed to digital data which is generated by the private signature key of an entity (a private signature key) and establishes the owner of the signature key (the entity) and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority.
<b>Digital Tachograph</b>	Recording Equipment.
<b>Digital Tachograph System</b>	Equipment, people or organisations, involved in any way with the recording equipment and tachograph cards.
<b>Entity</b>	A device connected to the VU
<b>Equipment Level</b>	At the equipment level, one single key pair (EQTj.SK and EQTj.PK) is generated and inserted in each equipment unit (vehicle unit or tachograph card). Equipment public keys are certified by a Member State Certification Authority (EQTj.C). This key pair is used for (i) authentication between vehicle units and tachograph cards, (ii) enciphering services: transport of session keys between vehicle units and tachograph cards, and (iii) digital signature of data downloaded from vehicle units or tachograph cards to external media.  The final master key $K_m$ and the identification key $K_{ID}$ are used for authentication between the vehicle unit and the motion sensor as well as


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						6 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

Term	Explanation
	<p>for an encrypted transfer of the motion sensor individual pairing key <math>K_P</math> from the motion sensor to the vehicle unit. The master key <math>K_m</math>, the pairing key <math>K_P</math> and the identification key <math>K_{ID}</math> are used merely during the pairing of a motion sensor with a vehicle unit (see [16844-3] for further details).</p> <p><math>K_m</math> and <math>K_{ID}</math> are permanently stored neither in the motion sensor nor in the vehicle unit; <math>K_P</math> is permanently stored in the motion sensor and temporarily – in the vehicle unit.</p>
<b>ERCA Policy</b>	<p>The ERCA policy is not a part of the Commission Regulation 1360/2002 [1360] and represents an important additional contribution. It was approved by the European Authority. The ERCA policy is available from the web site <a href="http://dtc.jrc.it">http://dtc.jrc.it</a>.</p> <p>Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.</p>
<b>European Authority</b>	<p>An organisation being responsible for the European Root Certification Authority policy. It is represented by</p> <p>European Commission            Directorate General for Transport and Energy            Unit E1 – Land Transport Policy            Rue de Mot, 24            B-1040 Bruxelles</p> <p>The entire Digital Tachograph System is operated in the frame and on the base of the Digital Tachograph System European Root Policy (Administrative Agreement TREN-E1-08-M-ST-SI2.503224 defining the general conditions for the PKI concerned and contains accordingly more detailed information.</p>
<b>European Root Certification Authority (ERCA)</b>	<p>An organisation being responsible for implementation of the ERCA policy and for the provision of key certification services to the Member States. It is represented by</p> <p>Digital Tachograph Root Certification Authority            Traceability and Vulnerability Assessment Unit            European Commission            Joint Research Centre, Ispra Establishment (TP.360)            Via E. Fermi, 1            I-21020 Ispra (VA)</p> <p>At the European level, ERCA generates a single European key pair (EUR.SK and EUR.PK). It uses the European private key to certify the Member States` public keys and keeps the records of all certified keys. A change of the European (root) key pair is currently not intended.</p> <p>ERCA also generates two symmetric partial master keys for the motion sensor: <math>K_{m_{WC}}</math> and <math>K_{m_{VU}}</math>. The first partial key <math>K_{m_{WC}}</math> is intended to be stored in each workshop tachograph card; the second partial key <math>K_{m_{VU}}</math> is</p>


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	
	Designation DTCO 1381 Security Target					
	Document key	Pages 7 of 106				
Villingen-Schwenningen (VIL)			Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Term	Explanation
	inserted into each vehicle unit. The final master key $K_m$ results from XOR (exclusive OR) operation between $K_{m_{wc}}$ and $K_{m_{vu}}$ .
<b>Identification data</b>	Identification data include VU identification data. Identification data are part of User data.
<b>Manufacturer</b>	The generic term for a VU Manufacturer producing and completing the VU to the TOE. The Manufacturer is the default user of the TOE during the manufacturing life phase.
<b>Management Device</b>	A dedicated device for software upgrade of the TOE
<b>Member State Authority (MSA)</b>	Each Member State of the European Union establishes its own national Member State Authority (MSA) usually represented by a state authority, e.g. Ministry of Transport. The national MSA runs some services, among others the Member State Certification Authority (MSCA).  The MSA has to define an appropriate Member State Policy (MSA policy) being compliant with the ERCA policy. MSA (MSA component personalisation service) is responsible for issuing of equipment keys, wherever these keys are generated: by equipment manufacturers, equipment personalisers or MSA itself.  MSA is also responsible for inserting data containing $K_{m_{wc}}$ , $K_{m_{vu}}$ , motion sensor identification and authentication data encrypted with $K_m$ and $K_{id}$ into respective equipment (workshop card, vehicle unit and motion sensor). Confidentiality, integrity and authenticity of the entities to be transferred between the different levels of the hierarchy within the tachograph system are subject to the ERCA and MSA policies.
<b>Member State Certification Authority (MSCA)</b>	At the Member State level, each MSCA generates a Member State key pair (MSi.SK and MSi.PK). Member States' public keys are certified by the ERCA (MSi.C). MSCAs use their Member State private key to certify public keys to be inserted in equipment (vehicle unit or tachograph card) and keep the records of all certified public keys with the identification of the equipment concerned. MSCA is allowed to change its Member State key pair. MSCA also calculates an additional identification key $K_{id}$ as XOR of the master key $K_m$ with a constant control vector CV. MSCA is responsible for managing and distributing $K_{m_{wc}}$ , $K_{m_{vu}}$ , motion sensor identification and authentication data encrypted with $K_m$ and $K_{id}$ to MSA component personalisation services.
<b>Motion data</b>	The data exchanged with the VU, representative of speed and distance travelled
<b>Motion Sensor</b>	Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled.
<b>Personal Identification</b>	A short secret password being only known to the approved workshops

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation		DTCO 1381 Security Target			
		Document key		Pages 8 of 106			
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			



# DTCO 1381 Security Target

Term	Explanation
<b>Number (PIN)</b>	
<b>Personalisation</b>	The process by which the equipment-individual data (like identification data and authentication key pairs for VU and TC or serial numbers and pairing keys for MS) are stored in and unambiguously, inseparably associated with the related equipment.
<b>Physically separated parts</b>	Physical components of the vehicle unit that are distributed in the vehicle as opposed to physical components gathered into the vehicle unit casing.
<b>Reference data.</b>	Data enrolled for a known identity and used by the verifier to check the verification data provided by an entity to prove this identity in an authentication attempt
<b>Secure messaging in combined mode</b>	Secure messaging using encryption and message authentication code according to [ISO 7816-4]
<b>Security data</b>	The specific data needed to support security enforcing functions (e.g. cryptographic keys). Security data are part of the sensitive data
<b>Sensitive data</b>	Data stored by the recording equipment and by the tachograph cards that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data
<b>SW-Upgrade</b>	Software-Upgrade installs a new version of software in the TOE.
<b>Tachograph cards</b>	Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types: <ul style="list-style-type: none"> <li>- driver card,</li> <li>- control card,</li> <li>- workshop card,</li> <li>- Company card.</li> </ul> A tachograph card possesses valid credentials for its authentication and their validity is verifiable. Valid credentials are a certified key pair for authentication being verifiable up to EUR.PK <sup>1</sup>
<b>TSF data</b>	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [CC]).
<b>Unknown equipment</b>	A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable. Valid credentials can be either a certified key pair for authentication of a device <sup>1</sup> or MS serial


<sup>1</sup> for tachograph cards, cf. [3821\_IB\_11], sec. 3.1

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com		2015-02-11		I CVAM TTS LRH		
		• Designation		DTCO 1381 Security Target			
		Document key		Pages 9 of 106			
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Term	Explanation
	number encrypted with the identification key ( $Enc(K_{ID} N_S)$ ) together with pairing key encrypted with the master key ( $Enc(K_m K_P)$ ). <sup>2</sup>
<b>Unknown User.</b>	not authenticated user
<b>Update issuer</b>	An organisation issuing the completed update data of the tachograph application
<b>User</b>	<p>Users are to be understood as legal human user of the TOE. The legal users of the VU comprise drivers, controllers, workshops and companies. User authentication is performed by possession of a valid tachograph card.</p> <p>There can also be Unknown User of the TOE and malicious user of the TOE</p> <p>– an attacker.</p> <p>User identity is kept by the VU in form of a concatenation of User group and User ID, cf. 3821_IB_10][9], UIA_208 representing security attributes of the role 'User'.</p>
<b>User data</b>	<p>Any data, other than security data (sec. III.12.2 of [3821_IB]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [3821_IB].</p> <p>User data are part of sensitive data.</p> <p>User data include identification data and activity data.</p> <p>CC give the following generic definitions for user data:</p> <p>Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [CC]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning (CC part 2 [CC]).</p>
<b>Vehicle Unit</b>	The recording equipment excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of this regulation
<b>Verification data</b>	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity

<sup>2</sup> for motion sensor, cf. [16844-3]


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com		2015-02-11		I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						10 of 106	
Villingen-Schwenningen (VIL)			Copyright ( C ) Continental AG 2008				

# DTCO 1381 Security Target

## 3.2 Abbreviations

Term/Abbreviation	Explanation
<b>CA</b>	Certification Authority
<b>CAN</b>	Controller Area Network
<b>CBC</b>	Cipher Block Chaining (an operation mode of a block cipher; here of TDES)
<b>CC</b>	Common criteria
<b>CCMB</b>	Common Criteria Management Board
<b>DAT</b>	Data
<b>DES</b>	Data Encryption Standard (see FIPS PUB 46-3)
<b>DL</b>	Download
<b>DTCO</b>	Digital Tachograph
<b>EAL</b>	Evaluation Assurance Level (a pre-defined package in CC)
<b>EC</b>	European Community
<b>ECB</b>	Electronic Code Book (an operation mode of a block cipher; here of TDES)
<b>EQT<sub>j</sub>-C</b>	equipment certificate
<b>EQT<sub>j</sub>-SK</b>	equipment private key
<b>EQT<sub>j</sub>-PK</b>	equipment public key
<b>EUR.PK</b>	European public key
<b>ERCA</b>	European Root Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
<b>FIL</b>	File
<b>Fun</b>	Function
<b>GST</b>	Generic security target
<b>IMS</b>	Independent movement signal
<b>K<sub>m</sub></b>	Master key
<b>K<sub>m<sub>vu</sub></sub></b>	Part of the Master key, will manage the pairing between a motion sensor and the vehicle unit
<b>K<sub>vu</sub></b>	Individual device key used to calculate MACs for the data integrity control of user data records
<b>K<sub>p</sub></b>	Pairing key of the motion sensor
<b>K<sub>sm</sub></b>	Session key between motion sensor and vehicle unit


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target				Document key	
Villingen-Schwenningen (VIL)						Copyright ( C ) Continental AG 2008	
						Pages 11 of 106	

# DTCO 1381 Security Target

Term/Abbreviation	Explanation
<b>K<sub>st</sub></b>	Session key between tachograph cards and vehicle unit
<b>kt</b>	transport key software upgrade
<b>MAC</b>	Message Authentication Code
<b>MD</b>	Management Device
<b>MS</b>	Motion Sensor
<b>MSA</b>	Member State Authority
<b>MSCA</b>	Member State Certification Authority (see Administrative Agreement 17398-00-12 (DG-TREN))
<b>MS<sub>i</sub>.C</b>	Member State certificate
<b>n.a.</b>	Not applicable
<b>OSP</b>	Organisational security policy
<b>PIN</b>	Personal Identification Number
<b>PKI</b>	Public Key Infrastructure
<b>PP</b>	Protection profile
<b>REQ xxx</b>	Requirement number in [3821_IB]
<b>RTC</b>	Real time clock
<b>ST</b>	Security Target
<b>SAR</b>	Security assurance requirements
<b>SFR</b>	Security functional requirement
<b>SFP</b>	Security Function Policy
<b>ST</b>	Security Target
<b>TBD</b>	To Be Defined
<b>TC</b>	Tachograph Card
<b>TDES</b>	Triple Data Encryption Standard (see FIPS PUB 46-3)
<b>TOE</b>	Target Of Evaluation
<b>TSF</b>	TOE security functionality
<b>UDE</b>	User Data Export
<b>VU</b>	Vehicle Unit

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						12 of 106	
Villingen-Schwenningen (VL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

## 4 ST Introduction

This document contains a description of the digital Tachograph DTCO 1381 Rel. 2.2 (the TOE), of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the security requirements. It states the claimed minimum resistance against attacks of security functional requirements and the required level of assurance for the development and the evaluation.

This document is based on the Vehicle Unit Generic Security Target, which is described in Appendix 10 of Annex IB 3821\_IB\_10] of the European Regulation (EEC) No 3821/85 [3821] amended by the Council Regulation (EEC) No 2135/98 [2135] and the Council Regulation (EC) No. 1360/2002 [1360].The document states the security objectives on the environment and describes how they are implemented in the digital Tachograph DTCO 1381 Rel. 2.2.

Requirements referred to in the document, are those of the body of Annex IB [3821\_IB]. For clarity of reading, duplication sometimes arises between Annex IB body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex IB body requirement referred by this security target requirement, the Annex IB body requirement shall prevail.

Annex IB body requirements not referred by security targets are not the subject of TSF. Unique labels have been assigned to threats, objectives, and procedural means and security requirements specifications for the purpose of traceability to development and evaluation documentation.

### 4.1 ST reference

**Title:** Digital Tachograph DTCO 1381 Security Target  
**Revision:** 1.17  
**Author:** Winfried Rogenz I CVAM TTS LRH  
**Publication date:** 11.02.2015

### 4.2 TOE reference

**Developer name:** Continental Automotive GmbH  
**TOE Name:** Digital Tachograph DTCO 1381  
**TOE Version number:** Release 2.2


### 4.3 TOE overview

#### 4.3.1 TOE definition and operational usage

The digital Tachograph DTCO 1381 Rel. 2.2 is a vehicle unit (VU) in the sense of Annex IB [3821\_IB] intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. It is connected to a motion sensor with which it exchanges vehicle's motion data.

The VU records and stores user activities data in its internal data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices. . It is connected to a motion sensor with which it exchanges vehicle's motion data. Users identify themselves to the VU using tachograph cards.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages 13 of 106			
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

The physical scope of the TOE is a device<sup>3</sup> to be installed in a vehicle. The TOE consists of a hardware box (includes a processing unit, a data memory, a real time clock, two smart card interface devices (driver and co-driver), a printer, a display, a visual warning, a calibration/downloading connector, and facilities for entry of user's inputs and embedded software) and of related user manuals. It must be connected to a motion sensor (MS) and to a power supply unit. It can temporarily be connected with other devices used for calibration, data export, software upgrade, and diagnostics.

The TOE receives motion data from the motion sensor and activity data via the facilities for entry of user's. It stores all this user data internally and can export them to the tachograph cards inserted, to the display, to the printer, and to electrical interfaces.

The TOE itself is depicted in the following figure (it shall be noted that although the printer mechanism is part of the TOE, the paper document once produced is not):

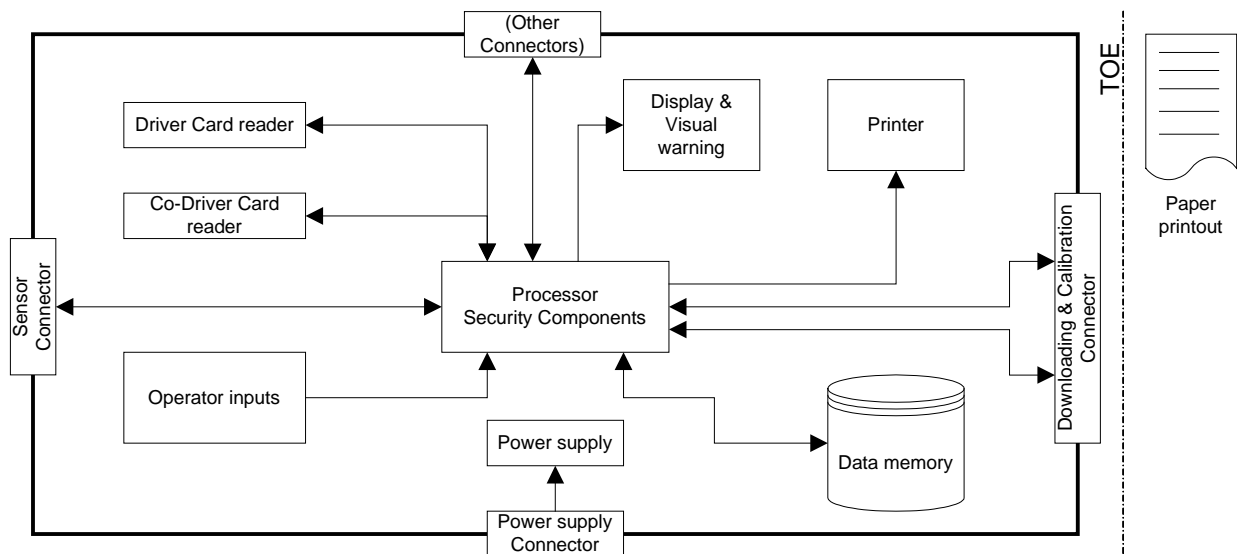



Figure 1 Digital Tachograph DTCO 1381

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

<sup>3</sup> single or physically distributed device

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target		Document key		Pages 14 of 106	
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

## 4.3.2 TOE major security features for operational use

The main security features of the TOE is as specified in 3821\_IB\_10]<sup>4</sup>: The data to be measured<sup>5</sup> and recorded and then to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.

It concretely means that security of the VU aims to protect

- a) the data recorded and stored in such a way as to prevent unauthorised access to and manipulation of the data and detecting any such attempts,
- b) the integrity and authenticity of data exchanged between the motion sensor and the vehicle unit,
- c) the integrity and authenticity of data exchanged between the recording equipment and the tachograph cards, and
- d) the integrity and authenticity of data downloaded.

The main security feature stated above is provided by the following major security services (please refer to 3821\_IB\_10], chap. 4):


- a) TOE\_SS.Identification\_Authentication (of motion sensor, tachograph cards and management devices),
- b) TOE\_SS.Access (Access control to functions and stored data),
- c) TOE\_SS.Accountability (Accountability of users),
- d) TOE\_SS.Audit (Audit of events and faults),
- e) TOE\_SS.Object\_Reuse (Object reuse for secret data),
- f) TOE\_SS.Accuracy (Accuracy of recorded and stored data),
- g) TOE\_SS.Reliability (Reliability of services),
- h) TOE\_SS.Data\_Exchange (Data exchange with motion sensor, tachograph cards and external media (download function)).

**Application Note 1** At least two services listed above – TOE\_SS.Identification\_Authentication as well as TOE\_SS.Data\_Exchange require TOE\_SS.Cryptographic\_support according to [3821\_IB\_10], sec. 4.9.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

<sup>4</sup> O.VU\_Main

<sup>5</sup> in the sense 'collected'; the physical data measurement is performed by the motion sensor being not part of the current TOE.

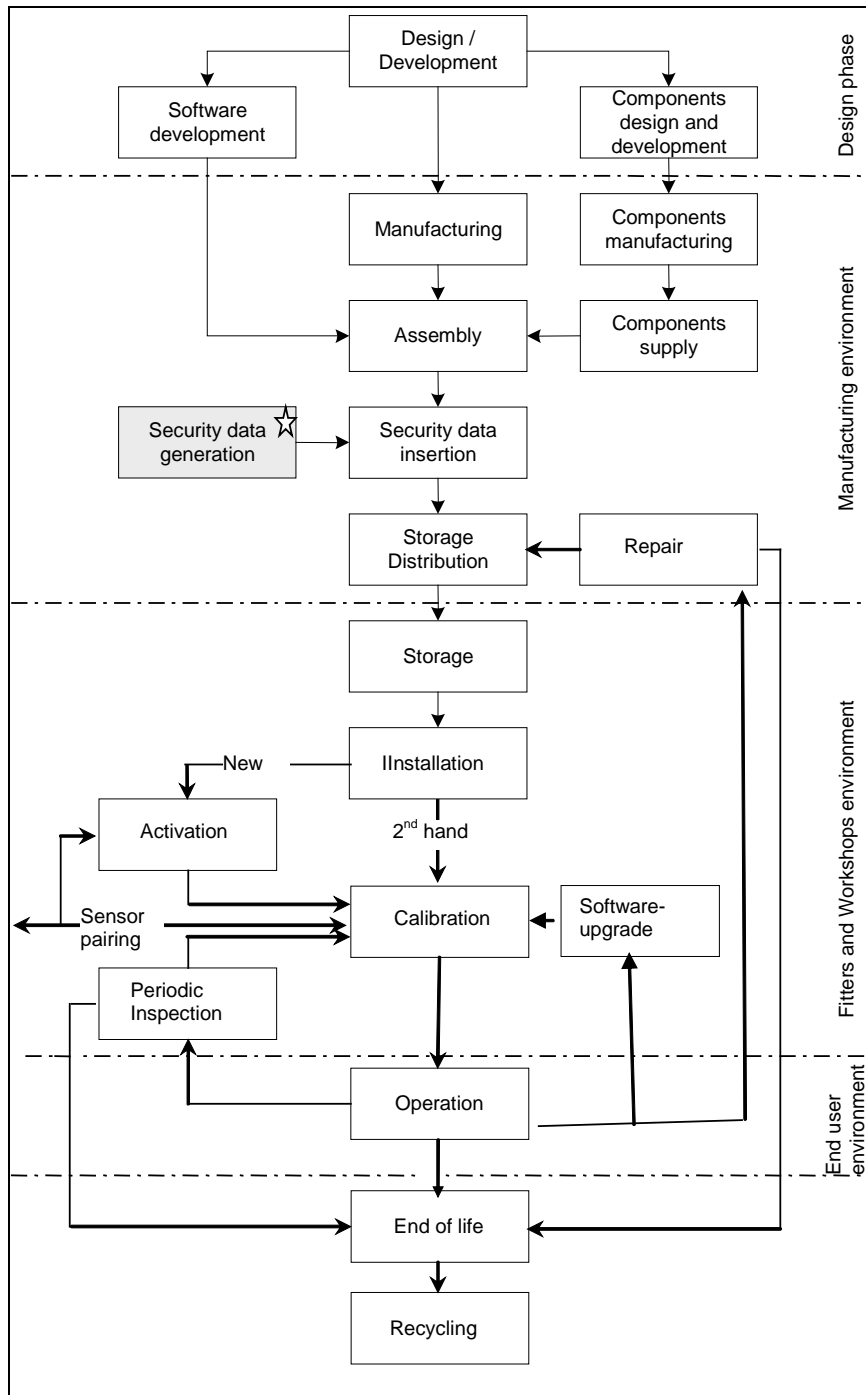
Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
Document key						Pages	
Villingen-Schwenningen (VIL)						15 of 106	
Copyright ( C ) Continental AG 2008							

# DTCO 1381 Security Target

## 4.3.3 TOE Type


The TOE type -digital Tachograph DTCO 1381 Rel. 2.2- is a vehicle unit (VU) in the sense of Annex IB [3821\_IB].

The typical life cycle of the VU is described in the following figure:



**Figure 2 Life Cycle of the DTCO 1381**

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target				Pages 16 of 106	
Villingen-Schwenningen (VIL)		Document key					
Copyright (C) Continental AG 2008							



# DTCO 1381 Security Target

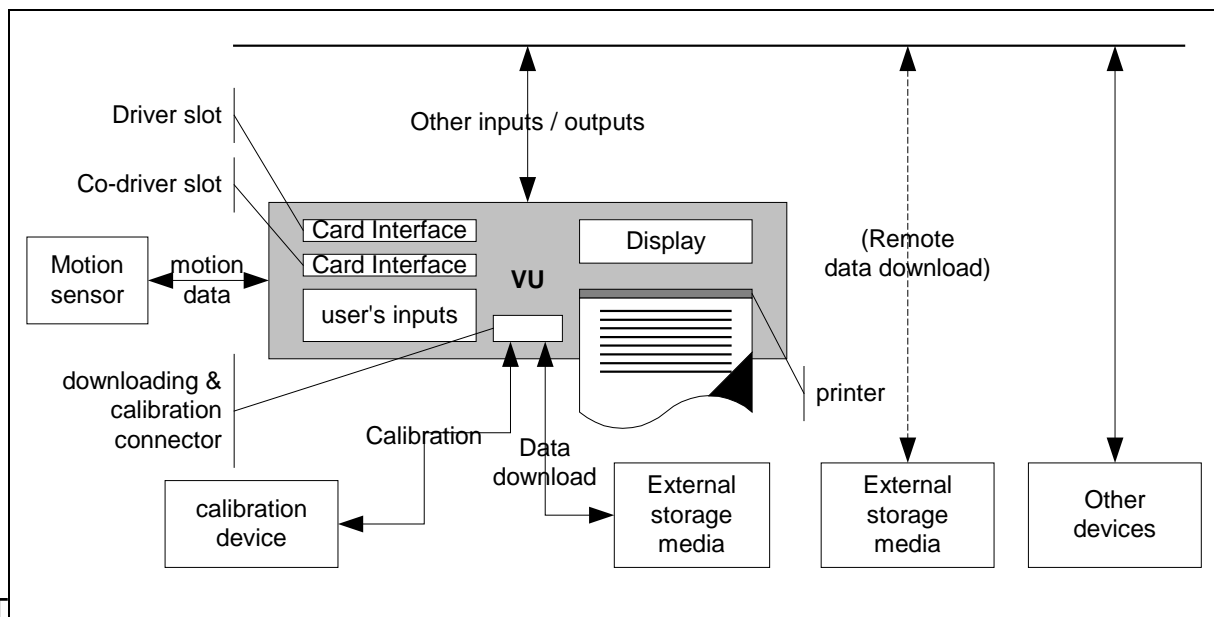
**Application Note 2** For the TOE a repair in the fitters and workshop environments is not planned. . An approved software upgrade can also be performed in the workshop environment.

**Application Note 3** The security requirements in sec. 4 of 3821\_IB\_10] limit the scope of the security examination of the TOE to the *operational phase* in the end user environment. Therefore, the security policy defined by the current security target also focuses on the *operational phase* of the VU in the end user environment. Some single properties of the *calibration phase*<sup>6</sup> being significant for the security of the TOE in its operational phase are also considered by the current ST as required by 3821\_IB\_10]. The TOE distinguishes between its calibration and operational phases by modes of operation as defined in [3821\_IB], REQ007 and REQ010: operational, control and company modes presume the operational phase, whereby the calibration mode presumes the calibration phase of the VU.

A security evaluation/certification involves all life phases into consideration to the extent as required by the assurance package chosen here for the TOE (see chap. 5.3 below). Usually, the TOE delivery from its manufacturer to the first customer (approved workshops) exactly happens at the transition from the *manufacturing* to the *calibration phase*.

### 4.3.4 Non-TOE hardware/software/firmware

The TOE operational environment while installed is depicted in the following figure:




**Figure 3 VU operational environment**

The following TOE external components are

- a) *mandatory* for a proper TOE operation
  - power supply e.g. from the vehicle where the TOE is installed
  - motion sensor

<sup>6</sup> calibration phase comprises all operations within the fitters and workshop environment

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
Document key				Pages		17 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

- b) *functionally necessary* for an Annex I B compliant operation
  - calibration device (fitters and workshops environment only)
  - tachograph cards (four different types of them)
  - printer paper
  - external storage media for data download
- c) *helpful* for a convenient TOE operation
  - connection to the vehicle network e.g. CAN-connection inter allia for the independent movement signal according to Req. 019a.

**Application Note 4** While operating, the TOE will verify, whether the motion sensor and tachograph cards connected possess appropriate credentials showing their belonging to the digital tachograph system. A security certification according to 3821\_IB\_10] is a prerequisite for the type approval of a motion sensor and tachograph cards.

## 5 Conformance claims

### 5.1 CC conformance claim

This security target claims conformance to:

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 [CC\_1]

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012 [CC\_2]

Common Criteria for Information Technology Security Evaluation, Part3: Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2012 [CC3]

as follows

- Part 2 conformant.
- Part 3 conformant.

The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012 [CEM] has to be taken into account.

### 5.2 PP conformance claim


This ST is conformant to the following documents:

[PP] Common Criteria Protection Profile, Digital Tachograph – Vehicle Unit (VU PP), BSI-CC-PP-0057, Version 1.0, 13<sup>th</sup> July 2010, Bundesamt für Sicherheit in der Informationstechnik,

**Application Note 5** This vehicle unit ST covers all requirements of the vehicle unit generic ITSEC ST as contained in 3821\_IB\_10]. The coverage of the requirements of 3821\_IB\_10] by the security functional requirements of the current ST is stated in Annex A, chap. 12 of this security target.

### 5.3 Package claim

This ST is conformant to the following security requirements package:

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 18 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target


---

Assurance package E3hCC31\_AP , as defined in section 9.2 below.

This assurance package is commensurate with [[JIL] defining an assurance package called E3hAP. This assurance package declares assurance equivalence between the assurance level E3 of an ITSEC certification and the assurance level of the package E3hAP within a Common Criteria (ver. ) certification (in conjunction with the Digital Tachograph System).

The assurance package E3hCC31\_AP represents the standard assurance package EAL4 augmented by the assurance components ATE\_DPT.2 and AVA\_VAN.5 (see sec. 9.2 below).

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
Document key					Pages 19 of 106		
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

## 6 Security problem definition

### 6.1 Introduction

#### Assets

The primary assets to be protected by the TOE as long as they are in scope of the TOE are (please refer to the glossary in chap.3 for the term definitions).

Object No.	Asset	Definition	Generic security property to be maintained by the current security policy
1	user data (recorded or stored in the TOE)	Any data, other than security data (sec. III.12.2 of [3821_IB]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [3821_IB].	Integrity Authenticity
2	user data transferred between the TOE and an external device connected	All user data being transferred from or to the TOE. A TOE communication partner can be: - a motion sensor, - a management device to transmit the upgrade file - a tachograph card, or - an external medium for data download. Motion data are part of this asset. User data can be received and sent (exchange ⇔ {receive, send}).	Confidentiality <sup>7</sup> Integrity Authenticity <sup>8</sup>


Table 1: Primary assets

All these primary assets represent User Data in the sense of the CC.

The secondary assets also having to be protected by the TOE in order to achieve a sufficient protection of the primary assets are:

<sup>7</sup> Not each data element being transferred represents a secret. Whose data confidentiality shall be protected while transferring them (i) between the TOE and a MS, is specified in [12], sec. 7.6 (instruction #11); (ii) between the TOE and a tachograph card – in [8], chap. 4 (access condition = PRO SM). Confidentiality of data to be downloaded to an external medium shall not be protected.

<sup>8</sup> Not each data element being transferred shall be protected for its integrity and authenticity. Whose data integrity and authenticity shall be protected while transferring them (i) between the TOE and a MS, is specified in [16844-3], sec. 7.5 (instruction #80); (ii) between the TOE and a tachograph card – in [3821\_IB\_2], chap. 4 (access condition = AUT). Integrity and authenticity of data to be downloaded to an external medium shall always be protected.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				20 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					


# DTCO 1381 Security Target

Object No.	Asset	Definition	Property to be maintained by the current security policy
3	Accessibility to the TOE functions and data only for authorised subjects	Property of the TOE to restrict access to TSF and TSF-data stored in the TOE to authorised subjects only.	Availability
4	Genuineness of the TOE	Property of the TOE to be authentic in order to provide the claimed security functionality in a proper way.	Availability
5	TOE immanent secret security data	<p>Secret security elements used by the TOE in order to enforce its security functionality.</p> <p>There are the following security elements of this category:</p> <ul style="list-style-type: none"> <li>- equipment private key (EQT.SK), see [3821_IB], sec. III.12.2,</li> <li>- vehicle unit part of the symmetric master key for communication with MS (<math>K_{m_{VU}}</math>), see [3821_IB_11], sec. 3.1.3,</li> <li>- session key between motion sensor and vehicle unit <math>K_{Sm}</math> (see [16844-3], sec. 7.4.5 (instruction 42)),</li> <li>- session key between tachograph cards and vehicle unit <math>K_{St}</math> (see [3821_IB_11], sec. 3.2)</li> </ul> <p>transport key software upgrade kt</p>	Confidentiality Integrity
6	TOE immanent non-secret security data	<p>Non-secret security elements used by the TOE in order to enforce its security functionality.</p> <p>There are the following security elements of this category:</p> <ul style="list-style-type: none"> <li>- European public key (EUR.PK),</li> <li>- Member State certificate (MS.C),</li> <li>- equipment certificate (EQT.C).</li> </ul> <p>see [3821_IB], sec. III.12.2.</p>	Integrity Authenticity

**Table 2 Secondary assets**

**Application Note 6** The workshop tachograph card requires an additional human user authentication by presenting a correct PIN value to the card. The vehicle unit (i) transmits the PIN verification value input by the user to the card and (ii) receives the card response to this verification attempt. A workshop tachograph card can only be used within the fitters and workshops environment (see A.Card\_Availability below), which is presumed to be trustworthy (see A.Approved\_Workshops below). Hence, no threat agent is presumed while using a workshop tachograph card. In this context, the VU is not required to secure a PIN verification value and any card response to a verification attempt, cf. [3821\_IB\_11], chap. 4.

The secondary assets represent TSF and TSF-data in the sense of the CC.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 21 of 106	
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			


# DTCO 1381 Security Target

## Subjects and external entities

28 This security target considers the following subjects:

External Entity No.	Subject No.	Role	Definition
1	1	User	<p>Users are to be understood as legal human user of the TOE. The legal users of the VU comprise drivers, controllers, workshops and companies. User authentication is performed by possession of a valid tachograph card.</p> <p>There can also be Unknown User of the TOE and malicious user of the TOE – an attacker. User identity is kept by the VU in form of a concatenation of User group and User ID, cf. 3821_IB_10], UIA_208 representing security attributes of the role ‘User’.</p> <p>An attacker is a threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the assets having to be maintained.</p> <p>The attacker is assumed to possess an at most <i>high</i> attack potential.</p> <p>Please note that the attacker might ‘capture’ any subject role recognised by the TOE.</p> <p>Due to constraints and definitions in 3821_IB_10], an attacker is an <u>attribute</u> of the role ‘User’ in the context of the current ST. Being a legal user is also an attribute of the role User.</p>
2	2	Unknown User	not authenticated user.
3	3	Motion Sensor	<p>Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled.</p> <p>A MS possesses valid credentials for its authentication and their validity is verifiable. Valid credentials are MS serial number encrypted with the identification key (<math>Enc(K_{ID} N_S)</math>) together with pairing key encrypted with the master key (<math>Enc(K_m K_P)</math>)</p>
4	-	Tachograph Card	<p>Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types:</p> <p>driver card,</p>

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						22 of 106	
Villingen-Schwenningen (VIL)			Copyright ( C ) Continental AG 2008				

# DTCO 1381 Security Target

External Entity No.	Subject No.	Role	Definition
			control card, workshop card, company card. A tachograph card possesses valid credentials for its authentication and their validity is verifiable. Valid credentials are a certified key pair for authentication being verifiable up to EUR.PK.
5	4	Unknown equipment	A technical device not possessing valid credentials for its authentication or validity of its credentials is not verifiable. Valid credentials can be either a certified key pair for authentication of a device or MS serial number encrypted with the identification key (Enc(K <sub>ID</sub>  N <sub>S</sub> )) together with pairing key encrypted with the master key (Enc(K <sub>m</sub>  K <sub>p</sub> )).
-		- Attacker	see item User above.

**Table 3: Subjects and external entities**

**Application Note 7** This table defines the subjects in the sense of [CC] which can be recognised by the TOE independent of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entity – an ‘image’ inside and ‘works’ then with this TOE internal image (also called subject in [CC]). From this point of view, the TOE itself does not differ between ‘subjects’ and ‘external entities’. There is no dedicated subject with the role ‘attacker’ within the current security policy, whereby an attacker might ‘capture’ any subject role recognised by the TOE.


## 6.2 Threats

This section of the security problem definition describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of TOE’s use in the operational environment. The threats are identical to those given in 3821\_IB\_10] chapter 3.3.

### 6.2.1 Threats averted solely by the TOE

- T.Card\_Data\_Exchange** Users could try to modify data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal).
- T.Faults** Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security.<sup>9</sup>
- T.Output\_Data** Users could try to modify data output (print, display or download).<sup>9</sup>

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 23 of 106	
Villingen-Schwenningen (VL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

## 6.2.2 Threats averted by the TOE and its operational environment

<b>T.Access</b>	Users could try to access functions <sup>9</sup> not allowed to them (e.g. drivers gaining access to calibration function).
<b>T.Calibration_Parameters</b>	Users could try to use miscalibrated equipment <sup>9</sup> (through calibration data modification, or through organisational weaknesses).
<b>T.Clock</b>	Users could try to modify internal clock. <sup>9</sup>
<b>T.Design</b>	Users could try to gain illicit knowledge of design <sup>9</sup> either from manufacturer's material (through theft, bribery ...) or from reverse engineering.
<b>T.Environment</b>	Users could compromise the VU security <sup>9</sup> through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,...).
<b>T.Fake_Devices</b>	Users could try to connect fake devices (motion sensor, smart cards) to the VU. <sup>10</sup>
<b>T.Hardware</b>	Users could try to modify VU hardware. <sup>9</sup>
<b>T.Identification</b>	Users could try to use several identifications or no identification. <sup>11</sup>
<b>T.Motion_Data</b>	Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal). <sup>12</sup>
<b>T.Power_Supply</b>	Users could try to defeat the VU security objectives <sup>9</sup> by modifying (cutting, reducing, increasing) its power supply.
<b>T.Security_Data</b>	Users could try to gain illicit knowledge of security data <sup>13</sup> during security data generation or transport or storage in the equipment.
<b>T.Software</b>	Users could try to modify VU software. <sup>9</sup>
<b>T.Stored_Data</b>	Users could try to modify stored data (security <sup>14</sup> or user data).

<sup>9</sup> The terms 'miscalibrated equipment', 'VU security', 'VU security objectives', 'data output', 'not allowed functions', 'VU in a well defined state', 'VU design', 'correctness of the internal clock', 'integrity of VU hardware', 'integrity of the VU software', 'full activated security functionality of the VU' correspond with 3821\_IB\_10] and are covered by the assets 'Accessibility to the TOE functions and data only for authorised subjects' and 'Genuineness of the TOE'


<sup>10</sup> Communication with genuine/known equipment is a prerequisite for a secure data exchange and, hence, represents a partial aspect of the asset 'user data transferred between the TOE and an external device connected'.

<sup>11</sup> Identification data are part of the asset 'User data', see Glossary.

<sup>12</sup> Motion data transmitted are part of the asset 'user data transferred between the TOE and an external device connected'.

<sup>13</sup> 'security data' are covered by the assets 'TOE immanent secret security data' and 'TOE immanent non-secret security data'

<sup>14</sup> it means 'TOE immanent secret security data' and 'TOE immanent non-secret security data'

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 24 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			



# DTCO 1381 Security Target

**T.Tests** The use of non invalidated test modes or of existing back doors could compromise the VU security.

**Application Note 8** Threat T.Faults represents a ‘natural’ flaw not induced by an attacker; hence, no threat agent can be stated here.

The threat agent for T.Tests is User. It can be deduced from the semantic content of T.Tests.

## 6.2.3 Threats averted solely by the TOE’s operational environment

**T.Non\_Activated** Users could use non activated equipment.<sup>9</sup>

## 6.3 Organisational security policies

The TOE and/or its environment shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

They are defined here to reflect those security objectives from 3821\_IB\_10] for which there is no threat directly and fully associated.

### 6.3.1 OSPs related to the TOE

**OSP.Accountability** The VU must collect accurate accountability data.

**OSP.Audit** The VU must audit attempts to undermine system security and should trace them to associated users.

**OSP.Processing** The VU must ensure that processing of inputs to derive user data is accurate.


**OSP.Test\_Points** All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU must disabled or removed before the VU activation during the manufacturing process

### 6.3.2 OSPs related to the TOE and its operational environment

**OSP.Type\_Approved\_MS<sup>15</sup>** The VU shall only be operated together with a motion sensor being type approved according to Annex I (B).

**OSP.Management\_Device** The Management Device supports the appropriate communication interface with the VU and secures the relevant secrets inside the MD as appropriate.

<sup>15</sup> The identity data of the motion sensor (serial number Ns) will be sent to the VU on request by the MS itself (see instruction #40 in [16844-3]). The ‘certificate’ Enc(K<sub>ID</sub>|Ns) stored in the motion sensor is merely used by it for VU authentication, but not for verifying Ns by the VU (see instruction #41 in [16844-3]). Therefore, the VU accepts this data (serial number Ns) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				25 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

## 6.3.3 OSPs related to the TOE's operational environment

### OSP.PKI


- 1) The European Authority shall establish a PKI according to [3821\_IB\_11], sec. 3.1.1 (starting with ERCA). This PKI is used for device authentication (TOE <-> Tachograph Cards) and for digital signing the user data to be downloaded. The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of the PKI.
- 2) The ERCA shall securely generate its own key pair (EUR.PK and EUR.SK) and Member State certificates (MSi.C) over the public keys of the MSCAs.
- 3) The ERCA shall ensure that it issues MSi.C certificates only for the rightful MSCAs.
- 4) The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
- 5) MSCAs shall securely generate their own key pairs (MSi.PK and MSi.SK) and equipment certificates (EQTj.C) over the public keys of the equipment.
- 6) MSCAs shall ensure that they issue EQTj.C certificates only for the rightful equipment.

### OSP.MS\_Keys

- 1) The European Authority shall establish a special key infrastructure for management of the motion sensor keys according to [16844-3] (starting with ERCA). This key infrastructure is used for device authentication (TOE <-> MS). The European Authority shall properly operate the ERCA steering other levels (the Member State and the equipment levels) of this key infrastructure.
- 2) The ERCA shall securely generate both parts (K<sub>MVU</sub> and K<sub>MWC</sub>) of the master key (K<sub>M</sub>).
- 3) The ERCA shall ensure that it securely convey this key material only to the rightful MSCAs.
- 4) The ERCA shall issue the ERCA policy steering its own acting and requiring MSCAs to enforce at least the same rules.
- 5) MSCAs shall securely calculate the motion sensor identification key (K<sub>ID</sub>) and the motion sensor's credentials: MS individual serial number encrypted with the identification key (Enc(K<sub>ID</sub>|N<sub>S</sub>)) and MS individual pairing key encrypted with the master key (Enc(K<sub>M</sub>|K<sub>P</sub>)).
- 6) MSCAs shall ensure that they issue these MS credentials<sup>16</sup>, K<sub>MVU</sub><sup>17</sup> and K<sub>MWC</sub><sup>18</sup> only to the rightful equipment.

<sup>16</sup> to the motion sensors  
<sup>17</sup> to the vehicle units  
<sup>18</sup> to the workshop cards

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com		2015-02-11		I CVAM TTS LRH		
		Designation DTCO 1381 Security Target				Pages 26 of 106	
		Document key					
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

## 6.4 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.


The GST in 3821\_IB\_10] does not define any dedicated assumption, but measures; these measures will be reflected in the current ST in form of the security objectives for the TOE environment below.

Hence, it is to define some assumptions in the current ST being sensible and necessary from the formal point of view (to reflect those environmental measures from 3821\_IB\_10]).

<b>A.Activation</b>	Vehicle manufacturers and fitters or workshops activate the TOE after its installation before the vehicle leaves the premises where installation took place.
<b>A.Approved_Workshops</b>	The Member States approve, regularly control and certify trusted fitters and workshops to carry out installations, calibrations, checks, inspections, repairs.
<b>A.Card_Availability</b>	Tachograph cards are available to the TOE users and delivered by Member State authorities to authorised persons only.
<b>A.Card_Traceability</b>	Card delivery is traceable (white lists, black lists), and black lists are used during security audits.
<b>A.Controls</b>	Law enforcement controls will be performed regularly and randomly, and must include security audits and (as well as visual inspection of the equipment).
<b>A.Driver_Card_Uniqueness</b>	Drivers possess, at one time, one valid driver card only.
<b>A.Faithful_Calibration</b>	Approved fitters and workshops enter proper vehicle parameters in recording equipment during calibration.
<b>A.Faithful_Drivers</b>	Drivers play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected ...). <sup>19</sup>
<b>A.Regular_Inspections</b>	Recording equipment will be periodically inspected and calibrated.

<sup>19</sup> The assumption A.Faithful\_Drivers taken from the Generic Security Target 3821\_IB\_10] seems not to be realistic and enforceable, because the driver is the person, who has to be controlled and surveyed (see the Council Regulation [1360] This assumption is made in the current ST only for the sake of compatibility with the GST 3821\_IB\_10]. and is necessary from *functional* point of view.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation DTCO 1381 Security Target					
		Document key				Pages 27 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

## 7 Security objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment

### 7.1 Security objectives for the TOE

The following TOE security objectives address the protection provided by the TOE *independent* of the TOE environment.


They are derived from the security objectives of as defined in in 3821\_IB\_10] chapter 3.5.

<b>O.Access</b>	The TOE must control user access to functions and data.
<b>O.Accountability</b>	The TOE must collect accurate accountability data.
<b>O.Audit</b>	The TOE must audit attempts to undermine system security and should trace them to associated users.
<b>O.Authentication</b>	The TOE should authenticate users and connected entities (when a trusted path needs to be established between entities).
<b>O.Integrity</b>	The TOE must maintain stored data integrity.
<b>O.Output</b>	The TOE must ensure that data output reflects accurately data measured or stored.
<b>O.Processing</b>	The TOE must ensure that processing of inputs to derive user data is accurate.
<b>O.Reliability</b>	The TOE must provide a reliable service.
<b>O.Secured_Data_Exchange</b>	The TOE must secure data exchanges with the motion sensor and with tachograph cards.
<b>O.Software_Analysis<sup>20</sup></b>	There shall be no way to analyse or debug software <sup>21</sup> in the field after the TOE activation.
<b>O.Software_Upgrade</b>	The TOE must ensure authenticity and integrity of software to be installed during a software upgrade.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

<sup>20</sup> This objective is added for the sake of a more clear description of the security policy: In the GST [3821\_IB\_10]], this aspect is part of O.Reliability, what might be not self-evident. The special concern here is RLB\_204 in 3821\_IB\_10]

<sup>21</sup> It is a matter of the decision by the certification body and the evaluation facility involved in a concrete certification process on a classification of the TOE (hard- and software) into security relevant and irrelevant parts

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
		Designation				Pages	
		DTCO 1381 Security Target				28 of 106	
Document key				Copyright ( C ) Continental AG 2008			
Villingen-Schwenningen (VIL)							

# DTCO 1381 Security Target

## 7.2 Security objectives for the operational environment

The following security objectives for the TOE's operational environment address the protection provided by the TOE environment *independent* of the TOE itself.

They are derived from the security objectives as defined in 3821\_IB\_10] chapter 3.6, Where they are represented as security measures.

### 7.2.1 Design environment (cf. the life cycle diagram in Figure 2 above)

**OE.Development** VU developers shall ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.

### 7.2.2 Manufacturing environment

**OE.Manufacturing** VU manufacturers shall ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security.

**OE.Sec\_Data\_Generation** Security data generation algorithms shall be accessible to authorised and trusted persons only.

**OE.Sec\_Data\_Transport** Security data shall be generated, transported, and inserted into the TOE, in such a way to preserve its appropriate confidentiality and integrity.

**OE.Delivery** VU manufacturers, vehicle manufacturers and fitters or workshops shall ensure that handling of the TOE is done in a manner which maintains IT security.

**OE.Software\_Upgrade** Software revisions shall be granted security certification before they can be implemented in the TOE.


**OE.Sec\_Data\_Strong<sup>22</sup>** Security data inserted into the TOE shall be cryptographically strong as required by [3821\_IB\_11].

**OE.Test\_Points<sup>23</sup>** All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation by the VU manufacturer during the manufacturing process.

**Application Note 9** Please note that the design and the manufacturing environments are not the intended usage environments for the TOE (cf. the *Application Note 3* above).

<sup>22</sup> The security objective OE.Sec\_Data\_Strong is defined in addition to 3821\_IB\_10] in order to reflect an aim of establishing the PKI and the symmetric key infrastructure (OSP.PKI and OSP.MS\_Keys)

<sup>23</sup> this objective is added for the sake of a more clear description of the security policy: In the GST 3821\_IB\_10], this aspect is part of O.Reliability, what might be not self-evident: A TOE cannot achieve an objective depending on action of its manufacturer. The special concern here is RLB\_201 in 3821\_IB\_10].

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 29 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

The security objectives for these environments being due to the current security policy (OE.Development, OE.Manufacturing, OE.Test\_Points, OE.Delivery) are the subject to the assurance class ALC. Hence, the related security objectives for the design and the manufacturing environments do not address any potential *TOE user* and, therefore, cannot be reflected in the documents of the assurance class AGD.

The remaining security objectives for the manufacturing environment (OE.Sec\_Data\_Generation, OE.Sec\_Data\_Transport, OE.Sec\_Data\_Strong and OE.Software\_Upgrade) are subject to the ERCA and MSA Policies and, therefore, are not specific for the TOE.

## 7.2.3 Fitter and workshops environment


- OE.Activation** Vehicle manufacturers and fitters or workshops shall activate the TOE after its installation before the vehicle leaves the premises where installation took place.
- OE.Approved\_Workshops** Installation, calibration and repair of recording equipment shall be carried by trusted and approved fitters or workshops.
- OE.Faithful\_Calibration** Approved fitters and workshops shall enter proper vehicle parameters in recording equipment during calibration.
- OE.Management\_Device** The Management Device (MD) is installed in the approved workshops according to A.Approved\_Workshops. The software upgrade data and necessary key data (for the software upgrade) are imported into the MD by the approved workshops according to A.Approved\_Workshops.

## 7.2.4 End user environment

- OE.Card\_Availability** Tachograph cards shall be available to TOE users and delivered by Member State Authorities to authorised persons only.
- OE.Card\_Traceability** Card delivery shall be traceable (white lists, black lists), and black lists must be used during security audits.
- OE.Controls** Law enforcement controls shall be performed regularly and randomly, and must include security audits.
- OE.Driver\_Card\_Uniqueness** Drivers shall possess, at one time, one valid driver card only.
- OE.Faithful\_Drivers<sup>24</sup>** Drivers shall play by the rules and act responsibly (e.g. use their driver cards; properly select their activity for those that are manually selected ...).
- OE.Regular\_Inspections** Recording equipment shall be periodically inspected and calibrated.

<sup>24</sup> The objective OE.Faithful\_Drivers taken from the Generic Security Target 3821\_IB\_10] seems not to be realistic and enforceable, because the driver is the person, who has to be controlled and surveyed (see the Council Regulation [1360]). This objective is claimed in the current ST only for the sake of compatibility with the GST 3821\_IB\_10] and is necessary from a *functional* point of view, see also A.Faithful\_Drivers.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				30 of 106	
Document key				Copyright ( C ) Continental AG 2008			
Villingen-Schwenningen (VIL)							


# DTCO 1381 Security Target

**OE.Type\_Approved\_MS<sup>25</sup>**

The Motion Sensor of the recording equipment connected to the TOE shall be type approved according to Annex I (B).

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

<sup>25</sup> The identity data of the motion sensor (serial number  $N_S$ ) will be sent to the VU on request by the MS itself (see instruction #40 in [16844-3]). The 'certificate'  $Enc(K_{ID}|N_S)$  stored in the motion sensor is merely used by it for VU authentication, but not for verifying NS by the VU (see instruction #41 in [16844-3]). Therefore, the VU accepts this data (serial number  $N_S$ ) as it is. Hence, the structure of the motion sensor Identification Data is the matter of the IT environment (here: MS), but not of the VU itself. A correct structure of the MS identity is guaranteed by the fact that the MS is type approved (-> UIA\_202).

	Date	Department	Sign
Designed by	winfried.rogenz@continental-corporation.com	2015-02-11	I CVAM TTS LRH
Released by	winfried.rogenz@continental-corporation.com	2015-02-11	I CVAM TTS LRH
		Designation DTCO 1381 Security Target	Pages 31 of 106
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008	

# DTCO 1381 Security Target


## 1 7.3 Security objectives rationale

2 The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for *sufficiency* and  
 3 *necessity* of the security objectives defined. It shows that all threats and OSPs are addressed by the security objectives. It also shows that all  
 4 assumptions are addressed by the security objectives for the TOE environment.

5 This rationale covers the rationale part in 3821\_IB\_10] chapter 8.

6


	Threats															OSPs						Assumptions														
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.PKI	OSP.MS_Keys	OSP.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections	
O.Access	X					X	X		X							X		X																		
O.Accountability		X																X																		
O.Audit	X	X				X			X	X	X		X	X			X	X		X																
O.Authentication	X	X				X	X		X		X											X														
O.Integrity						X											X																			

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
Villingen-Schwenningen (VIL)						32 of 106	
Copyright (C) Continental AG 2008							




# DTCO 1381 Security Target

	Threats													OSPs					Assumptions																	
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.PKI	OSP.MS_Keys	OSP.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections	
O.Output					x					x			x			x	x																			
O.Processing						X	x	X	x	x	x					x	x				x															
O.Reliability			x	X	x			x	x	x	x				x	x	x	x				x														
O.Secured_Data_Exchange							x			x		X				x																				
O.Software_Analysis						x																														
O.Software_Upgrade																	x										x									
OE.Development						x											x																			
OE.Software_Upgrade																x	x	x																		

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						33 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					


# DTCO 1381 Security Target

	Threats															OSPs					Assumptions																	
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.PKI	OSP.MS_Keys	OSP.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections			
OE.Delivery												x																										
OE.Manufacturing				X	X																																	
OE.Sec_Data_Strong															x									X	X													
OE.Sec_Data_Generation															x									X	X													
OE.Sec_Data_Transport															x									x	X													
OE.Test.Points																						X																
OE.Activation	X											x															X											

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
Document key						Pages 34 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					

# DTCO 1381 Security Target

	Threats													OSPs						Assumptions																
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	OSP.Accountability	OSP.Audit	OSP.Processing	OSP.Test_Points	OSP.Type_Approved_MS	OSP.PKI	OSP.MS_Keys	OSP.Management_Device	A.Activation	A.Approved_Workshops	A.Card_Availability	A.Card_Traceability	A.Controls	A.Driver_Card_Uniqueness	A.Faithful_Calibration	A.Faithful_Drivers	A.Regular_Inspections	
OE.Approved_Workshops						X	X					X															X									
OE.Card_Availability	X																												X							
OE.Card_Traceability	X																													X						
OE.Controls						X	X	X	X	X		X	X	X	X	X	X	X													X					
OE.Driver_Card_Uniqueness	X																														X					
OE.Faithful_Calibration						X	X																										X			
OE.Management_device																										X										

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						35 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					




# DTCO 1381 Security Target

1 A detailed justification required for *suitability* of the security objectives to coup with the security  
 2 problem definition is given below.

- 3 • **T.Access** is addressed by O.Authentication to ensure the identification of the user, O.Access to  
 4 control access of the user to functions and O.Audit to trace attempts of unauthorised accesses.  
 5 OE.Activation The activation of the TOE after its installation ensures access of the user to  
 6 functions.
- 7 • **T.Identification** is addressed by O.Authentication to ensure the identification of the user,  
 8 O.Audit to trace attempts of unauthorised accesses. O.Accountability contributes to address  
 9 this threat by storing all activity carried (even without an identification) with the VU. The  
 10 OE.Driver\_Card\_Uniqueness, OE.Card\_Availability and OE.Card\_Traceability objectives, also  
 11 required from Member States by law, help addressing the threat.
- 12 • **T.Faults** is addressed by O.Reliability for fault tolerance. Indeed, if the TOE provides a  
 13 reliable service as required by O.Reliability, the TOE cannot experience uncontrollable internal  
 14 states. Hence, also each possible fault of the TOE will be controllable, i.e. the TOE will be in a  
 15 wellknown state at any time. Therefore, threats grounding in faults of the TOE will be  
 16 eliminated.
- 17 • **T.Tests** is addressed by O.Reliability and OE.Manufacturing. Indeed, if the TOE provides a  
 18 reliable service as required by O.Reliability and its security cannot be compromised  
 19 during the manufacturing process (OE.Manufacturing), the TOE can neither enter any  
 20 invalidated test mode nor have any back door. Hence, the related threat will be  
 21 eliminated.
- 22 • **T.Design** is addressed by OE.Development and OE.Manufacturing before activation, and after  
 23 activation by O.Software\_Analysis to prevent reverse engineering and by O.Output (RLB\_206)  
 24 to ensure that data output reflects accurately data measured or store. and O.Reliability  
 25 (RLB\_201, 204, 206).
- 26 • **T.Calibration\_Parameters** is addressed by O.Access to ensure that the calibration function is  
 27 accessible to workshops only and by O.Authentication to ensure the identification of the  
 28 workshop and by O.Processing to ensure that processing of inputs made by the workshop to  
 29 derive calibration data is accurate, by O.Integrity to maintain the integrity of calibration  
 30 parameters stored. Workshops are approved by Member States authorities and are therefore  
 31 trusted to calibrate properly the equipment (OE.Approved\_Workshops,  
 32 OE.Faithful\_Calibration). Periodic inspections and calibration of the equipment, as required by  
 33 law (OE.Regular\_Inspections), contribute to address the threat. Finally, OE.Controls includes  
 34 controls by law enforcement officers of calibration data records held in the VU, which helps  
 35 addressing the threat.
- **T.Card\_Data\_Exchange** is addressed by O.Secured\_Data\_Exchange. O.Audit contributes to  
 address the threat by recording events related to card data exchange integrity or authenticity  
 errors. O.Reliability (ACR\_201, 201a), O.Processing (ACR\_201a).
- **T.Clock** is addressed by O.Access to ensure that the full time adjustment function is accessible  
 to workshops only and by O.Authentication to ensure the identification of the workshop and by  
 O.Processing to ensure that processing of inputs made by the workshop to derive time

Transmittal, reproduction, dissemination and/or editing of this document  
 as well as utilization of its contents and communication thereof to  
 others without express authorization of the publisher will be  
 held liable for payment of damages. All rights reserved. Patent  
 registration of a utility model or design patent are reserved.


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages			
Villingen-Schwenningen (VIL)				37 of 106			
				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

1 adjustment data is accurate. Workshops are approved by Member States authorities and are  
 2 therefore trusted to properly set the clock (OE.Approved\_Workshops). Periodic inspections and  
 3 calibration of the equipment, as required by law (OE.Regular\_Inspections,  
 4 OE.Faithful\_Calibration), contribute to address the threat. Finally, OE.Controls includes controls  
 5 by law enforcement officers of time adjustment data records held in the VU, which helps  
 6 addressing the threat.

- 7 • **T.Environment:** is addressed by O.Processing to ensure that processing of inputs to derive  
 8 user data is accurate and by O.Reliability to ensure that physical attacks are countered.  
 9 OE.Controls includes controls by law enforcement officers of time adjustment data records held  
 10 in the VU, which helps addressing the threat.
- 11 • **T.Fake\_Devices** is addressed by o.Access (ACC\_205) O.Authentication (UIA\_201 – 205, 207  
 12 – 211, 213, UIA\_221 – 223), O.Audit (UIA\_206, 214, 220), O.Processing (ACR\_201a),  
 13 O.Reliability (ACR\_201, 201a), O.Secured\_Data\_Exchange (CSP\_201 - 205).  
 14 OE.Type\_Approved\_MS ensures that only motion sensors with correct identification data have  
 15 the credentials that are required to successfully authenticate themselves. OE.Controls and  
 16 OE.Regular\_Inspections help addressing the threat through visual inspection of the whole  
 17 installation.
- 18 • **T.Hardware** is mostly addressed in the user environment by O.Reliability, O.Output,  
 19 O.Processing and by O.Audit contributes to address the threat by recording events related to  
 20 hardware manipulation. The OE.Controls and OE.Regular\_Inspections help addressing the  
 21 threat through visual inspection of the installation.
- 22 • **T.Motion\_Data** is addressed by O.Authentication, O.Reliability (UIA\_206, ACR\_201, 201a),  
 23 O.Secured\_Data\_Exchange and OE.Regular\_Inspections, OE.Type\_Approved\_MS. O.Audit  
 24 contributes to address the threat by recording events related to motion data exchange integrity  
 25 or authenticity errors.
- 26 • **T.Non\_Activated** is addressed by the OE.Activation and OE.Delivery. Workshops are  
 27 approved by Member States authorities and are therefore trusted to activate properly the  
 28 equipment (OE.Approved\_Workshops). Periodic inspections and calibration of the equipment,  
 29 as required by law (OE.Regular\_Inspections, OE.Controls), also contribute to address the  
 30 threat.
- 31 • **T.Output\_Data** is addressed by O.Output. O.Audit contributes to address the threat by  
 32 recording events related to data display, print and download.
- 33 • **T.Power\_Supply** is mainly addressed by O.Reliability to ensure appropriate behaviour of the  
 34 VU against the attack. O.Audit contributes to address the threat by keeping records of attempts  
 35 to tamper with power supply. OE.Controls includes controls by law enforcement officers of  
 36 power supply interruption records held in the VU, which helps addressing the threat.  
 OE.Regular\_Inspections helps addressing the threat through installations, calibrations, checks,  
 inspections, repairs carried out by trusted fitters and workshops.
- **T.Security\_Data** is addressed by OE.Sec\_Data\_Generation, OE.Sec\_Data\_Strong,  
 OE.Sec\_Data\_Transport, OE.Software\_Upgrade, OE.Controls. It is addressed by the  
 O.Access, O.Processing, O.Secured\_Data\_Exchange to ensure appropriate protection while  
 stored in the VU. O.Reliability (REU\_201, RLB\_206).


Transmittal, reproduction, dissemination and/or editing of this document  
 as well as utilization of its contents and communication thereof to  
 others without express authorization of the holder of the rights  
 held liable for payment of damages. All terms, conditions, trade  
 registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				38 of 106	
		Document key					
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

- 1 • **T.Software** is addressed in the user environment by the O.Output, O.Processing, and
- 2 O.Reliability to ensure the integrity of the code. O.Audit contributes to address the threat by
- 3 recording events related to integrity errors. During design and manufacture, the threat is
- 4 addressed by the OE.Development objectives. O.Software\_Upgrade (integrity of the new SW).
- 5 OE.Controls, OE.Regular\_Inspections (checking for the audit records related).
- 6 • **T.Stored\_Data** is addressed mainly by O.Integrity, O.Access, O.Output and O.Reliability to
- 7 ensure that no illicit access to data is possible. The O.Audit contributes to address the threat by
- 8 recording data integrity errors. OE.Software\_Upgrade ,included that Software revisions shall be
- 9 security certified before they can be implemented in the TOE to prevent to alter or delete any
- 10 stored driver activity data. OE.Controls includes controls by law enforcement officers of
- 11 integrity error records held in the VU, which helps addressing the threat.
- 12 • **OSP.Accountability** is fulfilled by O.Accountability
- 13 • **OSP.Audit** is fulfilled by O.Audit.
- 14 • **OSP.Processing** is fulfilled by O.Processing.
- 15 • **OSP.Test\_Points** is fulfilled by O.Reliability and OE.Test\_Points
- 16 • **OSP.Type\_Approved\_MS** is fulfilled by O.Authentication and OE.Type\_Approved\_MS
- 17 • **OSP.PKI** is fulfilled by OE.Sec\_Data\_Generation, OE.Sec\_Data\_Strong,
- 18 OE.Sec\_Data\_Transport
- 19 • **OSP.MS\_Keys** is fulfilled by OE.Sec\_Data\_Generation, OE.Sec\_Data\_Strong,
- 20 OE.Sec\_Data\_Transport
- 21 • **OSP.Management\_Device** is fulfilled by O.Software\_Upgrade and OE.Management\_Device
- 22 • **A.Activation** is upheld by OE.Activation.
- 23 • **A.Approved\_Workshops** is upheld by OE.Approved\_Workshops.
- 24 • **A.Card\_Availability** is upheld by OE.Card\_Availability.
- 25 • **A.Card\_Traceability** is upheld by OE.Card\_Traceability.
- 26 • **A.Controls** is upheld by OE.Controls.
- 27 • **A.Driver\_Card\_Uniqueness** is upheld by OE.Driver\_Card\_Uniqueness.
- 28 • **A.Faithful\_Calibration** is upheld by OE.Faithful\_Calibration and OE.Approved\_Workshops.
- 29 • **A.Faithful\_Drivers** is upheld by OE.Faithful\_Drivers.
- 30 • **A.Regular\_Inspections** is upheld by OE.Regular\_Inspections.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent and/or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 39 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target


---

## 1 8 Extended components definition

### 2 8.1 Extended components definition

3  
4 This security target does not use any components defined as extensions to CC part 2.  
5

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				40 of 106	
		Document key					
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					



## 1 9 Security requirements

2 This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The  
 3 statement of **TOE security requirements** shall define the *functional* and *assurance* security  
 4 requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

5 The CC allows several operations to be performed on security requirements (on the component level);  
 6 *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 8.1 of Part 1 [CC\_1]] of the  
 7 CC. Each of these operations is used in this ST.

8 The **refinement** operation is used to add detail to a requirement, and, thus, further restricts a  
 9 requirement. Refinements of security requirements are denoted in such a way that added words are in  
 10 **bold text** and changed words are ~~crossed-out~~.

11 The **selection** operation is used to select one or more options provided by the CC in stating a  
 12 requirement. Selections having been made by the PP author are denoted as underlined text.  
 13 Selections to be filled in by the ST author appear in square brackets with an indication that a selection  
 14 is to be made, [selection:], and are *italicised*. Selections having been made by the ST author are  
 15 underlined and *italicised*.


16 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the  
 17 length of a password. Assignments having been made by the PP author are denoted by showing as  
 18 underlined text. Assignments to be filled in by the ST author appear in square brackets with an  
 19 indication that an assignment is to be made [assignment:], and are *italicised*. In some cases the  
 20 assignment made by the PP authors defines a selection to be performed by the ST author. Thus, this  
 21 text is underlined and italicised like *this*. Assignment having been made by the ST author are double  
 22 underlined and italicised.

23 The **iteration** operation is used when a component is repeated with varying operations. Iteration is  
 24 denoted by showing a slash “/”, and the iteration indicator after the component identifier. In order to  
 25 trace elements belonging to a component, the same slash “/” with iteration indicator is used behind the  
 26 elements of a component.

27 For the sake of a better readability, the author uses an additional notation in order to indicate belonging  
 28 of some SFRs to same functional cluster, namely a double slash “//” with the related functional group  
 29 indicator after the component identifier. In order to trace elements belonging to a component, the same  
 30 double slash “//” with functional cluster indicator is used behind the elements of a component.

### 9.1 Security functional requirements

The security functional requirements (SFRs) below are derived from the security enforcing functions (SEFs) specified in section 4 of the ITSEC vehicle unit GST in 3821\_IB\_10]. Each of the below SFRs includes in bold-face curly braces {...} a list of SEFs related. This not only explains why the given SFR has been chosen, but moreover is used to state further detail of the SFR without verbose repetition of the original text of the corresponding SEF(s) from 3821\_IB\_10]. The main advantage of this approach is avoiding redundancy, and, more important, any unambiguity.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 41 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization by Continental AG are prohibited. In particular, those persons with whom a confidentiality agreement has been concluded must be notified immediately in writing upon the first use of the information contained herein. For further information on our legal terms and conditions (including patent, copyright, trademark, and trade secret protection and other legal rights), please contact our Patent Department. All rights reserved.

# DTCO 1381 Security Target


1 The complete coverage of the SEF(s) from 3821\_IB\_10] is documented in Annex A, chap.12  
 2 below.

## 3 9.1.1 Overview

4 In order to give an overview of the security functional requirements in the context of the security  
 5 services offered by the TOE, the author of the ST defined the security functional groups and allocated  
 6 the functional requirements described in the following sections to them:

Security Functional Groups	Security Functional Requirements concerned
Identification and authentication of motion sensor und tachograph cards (according to 3821_IB_10], sec. 4.1)	<ul style="list-style-type: none"> <li>– FIA_UID.2/MS: Identification of the motion sensor</li> <li>– FIA_UID.2/TC: Identification of the tachograph cards</li> <li>– (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor</li> <li>– (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards</li> <li>– FIA_UAU.1/PIN: additional PIN authentication for the workshop card</li> <li>– FIA_AFL.1/MS: Authentication failure: motion sensor</li> <li>– FIA_AFL.1/TC: Authentication failure: tachograph cards</li> <li>– (FIA_ATD.1//TC, FMT_SMR.1//TC): User groups to be maintained by the TOE</li> </ul> <p>Supported by:</p> <ul style="list-style-type: none"> <li>– FCS_COP.1/TDES: for the motion sensor</li> <li>– FCS_COP.1/RSA: for the tachograph cards</li> <li>– (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management</li> <li>– FAU_GEN.1: Audit records: Generation</li> <li>– (FMT_MSA.1, FMT_SMF.1)</li> </ul>


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
	Document key	Pages 42 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008	

# DTCO 1381 Security Target

Security Functional Groups	Security Functional Requirements concerned
<p>Access control to functions and stored data (according to 3821_IB_10], sec. 4.2)</p>	<ul style="list-style-type: none"> <li>– (FDP_ACC.1/FIL, FDP_ACF.1/FIL): file structures</li> <li>– (FDP_ACC.1/FUN, FDP_ACF.1/FUN): functions</li> <li>– (FDP_ACC.1/DAT, FDP_ACF.1/DAT): stored data</li> <li>– (FDP_ACC.1/UDE, FDP_ACF.1/UDE): user data export</li> <li>– (FDP_ACC.1/IS, FDP_ACF.1/IS): input sources</li> </ul> <p>Supported by:</p> <ul style="list-style-type: none"> <li>– (FIA_UAU.2//MS, FIA_UAU.3/MS, FIA_UAU.6/MS): Authentication of the motion sensor</li> <li>– (FIA_UAU.1/TC, FIA_UAU.3/TC, FIA_UAU.5//TC, FIA_UAU.6/TC): Authentication of the tachograph cards</li> <li>– FIA_UAU.1/PIN: additional PIN authentication for the workshop card</li> <li>– FMT_MSA.3/FIL</li> <li>– FMT_MSA.3/FUN</li> <li>– FMT_MSA.3/DAT</li> <li>– FMT_MSA.3/UDE</li> <li>– FMT_MSA.3/IS</li> <li>– (FMT_MSA.1, FMT_SMF.1, FMT_SMR.1//TC)</li> </ul>
<p>Accountability of users (according to 3821_IB_10], sec. 4.3)</p>	<ul style="list-style-type: none"> <li>– FAU_GEN.1: Audit records: Generation</li> <li>– FAU_STG.1: Audit records: Protection against modification</li> <li>– FAU_STG.4: Audit records: Prevention of loss</li> <li>– FDP_ETC.2: Export of user data with security attributes</li> </ul> <p>Supported by:</p> <ul style="list-style-type: none"> <li>– (FDP_ACC.1/DAT, FDP_ACF.1/DAT): VU</li> </ul>


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com		2015-02-11		I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 43 of 106	
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Security Functional Groups	Security Functional Requirements concerned
	identification data – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): Data update on the TC – FPT_STM.1: time stamps – FCS_COP.1/TDES: for the motion sensor and the tachograph cards
Audit of events and faults (according to 3821_IB_10], sec. 4.4)	– FAU_GEN.1: Audit records: Generation – FAU_SAR.1: Audit records: Capability of reviewing Supported by: – (FDP_ACC.1/DAT, FDP_ACF.1/DAT): Storing motion sensor’s audit records – FDP_ETC.2 Export of user data with security attributes: Related audit records to the TC. FPT_PHP.1//Seal Passive detection of physical attack
Object reuse for secret data (according to 3821_IB_10], sec. 4.5)	– FDP_RIP.1 Subset residual information protection Supported by: – FCS_CKM.4: Cryptographic key destruction
Accuracy of recorded and stored data (according to 3821_IB_10], sec. 4.6)	– FDP_ITC.1: right input sources without sec. attributes (keyboard, calibration data, RTC) – FDP_ITC.2//IS: right input sources with sec. attributes (MS and TC) FDP_ITC.2/SW-Upgrade Import of user data with security attributes – FPT_TDC.1//IS: Inter-TSF basic TSF data consistency (MS and TC) – FDP_SDI.2: Stored data integrity Supported by: – (FDP_ACC.1/IS, FDP_ACF.1/IS): right input sources – (FDP_ACC.1/FUN, FDP_ACF.1/FUN):


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com		2015-02-11		I CVAM TTS LRH		
		• Designation		DTCO 1381 Security Target			
		Document key		Pages			
Villingen-Schwenningen (VIL)				44 of 106			
				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Security Functional Groups	Security Functional Requirements concerned
	limited manual entry – FAU_GEN.1: Audit records: Generation – FPT_STM.1: Reliable time stamps – (FIA_UAU.2//MS, FIA_UAU.3//MS, FIA_UAU.6//MS): Authentication of the motion sensor – (FIA_UAU.1//TC, FIA_UAU.3//TC, FIA_UAU.5//TC, FIA_UAU.6//TC): Authentication of the tachograph cards
Reliability of services (according to 3821_IB_10], sec. 4.7)	– FDP_ITC.2//IS: no executable code from external sources – FPR_UNO.1: Unobservability of leaked data – FPT_FLS.1: Failure with preservation of secure state FPT_PHP.1//Seal Passive detection of physical attack – FPT_PHP.2//Power_Deviation: Notification of physical attack – FPT_PHP.3: Resistance to physical attack: stored data – FPT_TST.1: TSF testing – FRU_PRS.1: Availability of services Supported by: – FAU_GEN.1: Audit records: Generation – (FDP_ACC.1//IS, FDP_ACF.1//IS): no executable code from external sources – (FDP_ACC.1//FUN, FDP_ACF.1//FUN): Tachograph Card withdrawal – FMT_MOF.1: No test entry points
Data exchange with motion sensor, tachograph cards and external media (download function) (according to 3821_IB_10], sec. 4.8)	– FCO_NRO.1: Selective proof of origin for data to be downloaded to external media – FDP_ETC.2 Export of user data with security attributes: to the TC and to external media

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
Document key			Pages 45 of 106
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008	

# DTCO 1381 Security Target

Security Functional Groups	Security Functional Requirements concerned
	– FDP_ITC.2//IS Import of user data with security attributes: from the MS and the TC Supported by: – FCS_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging) – FCS_COP.1/RSA: for data downloading to external media (signing) – (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4): cryptographic key management – (FDP_ACC.1/UDE, FDP_ACF.1/UDE): User data export to the TC and to external media – (FDP_ACC.1/IS, FDP_ACF.1/IS): User data import from the MS and the TC – FAU_GEN.1: Audit records: Generation
Management of and access to TSF and TSF-data	– The entire class FMT. Supported by: – the entire class FIA: user identification/authentication

## 1 Table 5 Security functional groups vs. SFRs

### 2 9.1.2 Class FAU Security Audit

#### 3 9.1.2.1 FAU\_GEN - Security audit data generation

4 **FAU\_GEN.1** Audit data generation {UIA\_206, UIA\_214, ACT\_201, ACT\_203, ACT\_204, ACT\_205,  
 5 AUD\_201, AUD\_202, AUD\_203, ACR\_205, RLB\_203, RLB\_206, RLB\_210, RLB\_214,  
 6 DEX\_202, DEX\_204}


Hierarchical to: -

Dependencies: FPT\_STM.1 Reliable time stamps: is fulfilled by FPT\_STM.1

**FAU\_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the not specified level of audit; and

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights reserved by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						46 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

1 c) the activities and auditable events specified in REQ 081, 084, 087, 090, 093, 094, 096, 098,  
 2 101, 102, 103, and 105a<sup>26,27</sup> and {UIA 206, UIA 214, ACR 205, ACT 201, ACT 203,  
 3 ACT 204, ACT 205, AUD 201, AUD 202, AUD 203, RLB 203, RLB 206, RLB 210,  
 4 RLB 214<sup>28</sup>, DEX 202, DEX 204}; *no other specifically defined audit events.*

5 **FAU\_GEN.1.2** The TSF shall record within each audit record at least the following information:

6 a) Date and time of the event, type of event, subject identity, and the outcome (success or failure)  
 7 of the event; and

8 b) For each audit event type, based on the auditable event definitions of the functional  
 9 components included in the ST, the information specified in {REQ 081, 084, 087, 090, 093, 094,  
 10 096, 098, 101, 102, 103, 105a 29}; *no other audit relevant information.*

## 11 9.1.2.2 FAU\_SAR - Security audit review

### 12 **FAU\_SAR.1** Audit review {AUD\_205}

Hierarchical to: -

Dependencies: FAU\_GEN.1 Audit data generation: is fulfilled by FAU\_GEN.1

13

14 **FAU\_SAR.1.1** The TSF shall provide everybody with the capability to read the recorded information  
 15 according to REQ 011 from the audit records.

16 **FAU\_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the  
 17 information.

## 18 9.1.2.3 FAU\_STG - Security audit event storage

### 19 **FAU\_STG.1** Protected audit trail storage {ACT\_206<sup>30</sup>}.

Hierarchical to: -

Dependencies: FAU\_GEN.1 Audit data generation: is fulfilled by FAU\_GEN.1

20 **FAU\_STG.1.1** The TSF shall protect the stored audit records in the audit trail from unauthorised dele-  
 21 tion.

22 **FAU\_STG.1.2** The TSF shall be able to detect unauthorised modifications to the stored audit records in  
 23 the audit trail.

### 24 **FAU\_STG.4** Prevention of audit data loss {ACT\_201, ACT\_206}<sup>31</sup>

Hierarchical to: FAU\_STG.3

Dependencies: FAU\_STG.1 Protected audit trail storage: is fulfilled by

26


27 all these REQ are referred to in {ACT\_201, ACT\_203, ACT\_204, ACT\_205, AUD\_201, AUD\_203}

28 Last card session not correctly closed

29 all these REQ are referred to in {ACT\_201, ACT\_203, ACT\_204, ACT\_205, AUD\_203}

30 REQ081 to 093 and REQ102 to 105a

31 REQ105b

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				47 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					

# DTCO 1381 Security Target

## FAU\_STG.1

1 **FAU\_STG.4.1** The TSF shall overwrite the oldest stored audit records and behave according to REQ  
 2 083, 086, 089, 092 and 105b if the audit trail is full.

3 **Application Note 10:** The data memory shall be able to hold 'driver card insertion and withdrawal  
 4 data' (REQ082), 'driver activity data' (REQ085) and 'places where daily work periods start and/or end'  
 5 (REQ088) for at least 365 days. Since these requirements are not subject to GST 3821\_IB\_10]<sup>32</sup>,  
 6 they are also not included in the formal content of FAU\_STG.4.

7 For same reason, the respective part of requirement for 'specific conditions data' (REQ105b,  
 8 at least 365 days) is also out of scope of the formal content of FAU\_STG.4.

### 9 9.1.3 Class FCO Communication

#### 10 9.1.3.1 FCO\_NRO Non-repudation of origin

##### 11 **FCO\_NRO.1** Selective proof of origin {DEX\_206, DEX\_207}

Hierarchical to: -

Dependencies: FIA\_UID.1 Timing of identification: not fulfilled, but **justified**

the components FIA\_UID.2/MS, FIA\_UID.2/TC being present in the ST do not fulfil this dependency, because they are not affine to DEX\_206, DEX\_207 (data download).

The sense of the current dependency would be to attach the VU identity (ACT\_202) to the data to be downloaded; the VU identification data are permanently stored in the VU, so that the VU always 'knows' its own identity.

12 **FCO\_NRO.1.1** The TSF shall be able to generate evidence of origin for transmitted data to be  
 13 downloaded to external media at the request of the originator.

14 **FCO\_NRO.1.2** The TSF shall be able to relate the VU identity of the information, and the data to be  
 15 downloaded to external media to which the evidence applies.

16 **FCO\_NRO.1.3** The TSF shall provide a capability to verify the evidence of origin of information to the  
 17 recipient given.

18 - according to specification [3821\_IB\_11], sec. 6.1,

19 no further limitation on the evidence of origin.

### 20 9.1.4 Class FCS Cryptographic Support


#### 9.1.4.1 FCS\_CKM - Cryptographic key management

##### **FCS\_CKM.1** Cryptographic key generation {CSP\_202}

Hierarchical to: -

Dependencies: [FCS\_CKM.2 Cryptographic key distribution or

<sup>32</sup> ACT\_206 does not require keeping data for at least 365 days

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 48 of 106	
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			




# DTCO 1381 Security Target

FCS\_COP.1 Cryptographic operation]: is fulfilled by FCS\_CKM.2;  
 FCS\_CKM.4 Cryptographic key destruction: is fulfilled by  
 FCS\_CKM.4

- 1 **FCS\_CKM.1.1** The TSF shall generate cryptographic keys in accordance with a specified
- 2 cryptographic key generation algorithm cryptographic key derivation algorithms (for
- 3 the session keys  $K_{sm}$ , and  $K_{st}$  as well as for the temporarily stored keys  $K_m$ ,  $K_p$ ,  $K_{ID}$
- 4 and  $K_t$ ) and specified cryptographic key sizes 112 bits that meet the following: list of
- 5 standards:

Key description	Algorithm and size	Standard, specification
<u>Motion sensor Master key <math>K_m</math> is temporarily stored key derived from the static key material within the workshop environment (OE.Approved Workshops) outside of the VU's operational phase</u>	<u>Two keys TDES key</u>	<u>[16844-3]</u>
<u>Pairing key of the motion sensor <math>K_p</math> is temporarily stored key derived from the static key material within the workshop environment (OE.Approved Workshops) outside of the VU's operational phase</u>	<u>Two keys TDES key</u>	<u>[16844-3]</u>
<u>motion sensor identification key <math>K_{ID}</math> is temporarily stored key derived from the static key material within the workshop environment (OE.Approved Workshops) outside of the VU's operational phase</u>	<u>Two keys TDES key</u>	<u>[16844-3]</u>
<u>Session key between motion sensor and vehicle unit <math>K_{sm}</math></u>	<u>Two keys TDES key</u>	<u>[16844-3]</u>
<u>session key between tachograph cards and vehicle unit <math>K_{st}</math></u>	<u>Two keys TDES key</u>	<u>[3821 IB 11], CSM 020</u>
<u><i><math>K_t</math> is temporarily stored key derived from the static key material within the workshop environment (OE.Approved Workshops) outside of the VU's operational phase</i></u>	<u><i>Two keys TDES key</i></u>	<u><i>As defined by the proprietary specification for the SW-Upgrade by the TOE developer</i></u>

## FCS\_CKM.2 Cryptographic key distribution {CSP\_203}

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages 49 of 106			
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Hierarchical to: -  
 Dependencies: [FDP\_ITC.1 or FDP\_ITC.2 or FCS\_CKM.1]: is fulfilled by FCS\_CKM.1  
 FCS\_CKM.4: is fulfilled by FCS\_CKM.4

1 **FCS\_CKM.2.1** The TSF shall distribute cryptographic keys in accordance with a specified  
 2 cryptographic key distribution method as specified in the table below that meets the  
 3 following list of standards.


Distributed key	Standard, specification
<u>session key between motion sensor and vehicle unit <math>K_{sm}</math></u>	<u>[16844-3], 7.4.5</u>
<u>session key between tachograph cards and vehicle unit <math>K_{st}</math></u>	<u>[3821 IB 11], CSM 020</u>

4  
 5 **FCS\_CKM.3** Cryptographic key access {**CSP\_204**}

Hierarchical to: -  
 Dependencies: [FDP\_ITC.1 or FDP\_ITC.2 or FCS\_CKM.1]:  
 a) fulfilled by FCS\_CKM.1 for the session keys  $K_{SM}$  and  $K_{ST}$  as well as for the temporarily stored keys  $K_m$ ,  $K_P$  and  $K_{ID}$ ;  
 b) fulfilled by FDP\_ITC.2//IS for the temporarily stored key  $K_{m_{wc}}$  (entry DEX\_203);  
 c) not fulfilled, but **justified** for EUR.PK, EQT.SK,  $K_{m_{vu}}$ : The persistently stored keys (EUR.PK, EQT.SK,  $K_{m_{vu}}$ ) will be loaded into the TOE outside of its operational phase, cf. also OE.Sec\_Data\_xx.  
 FCS\_CKM.4: is fulfilled by FCS\_CKM.4

6 **FCS\_CKM.3.1** The TSF shall perform cryptographic key access and storage in accordance with a  
 7 specified cryptographic key access method as specified below that meets the following list of  
 8 standards:

Key	key access method and specification
<u>Part of the Master key <math>K_{m_{wc}}</math></u>	<u>read out from the workshop card and temporarily stored in the TOE (calibration phase);</u>
<u>Motion sensor Master key <math>K_m</math></u>	<u>temporarily reconstructed from part of the Master key <math>K_{m_{vu}}</math> and part of the Master key <math>K_{m_{wc}}</math>, [3821 IB 11], CSM 036, CSM 037 (calibration phase);</u>
<u>motion sensor identification key <math>K_{ID}</math></u>	<u>temporarily reconstructed from the Master key <math>K_m</math> a motion sensor identification key <math>K_{ID}</math> as specified in [16844-3], sec. 7.2, 7.4.3</u>

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages 50 of 106			
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

# DTCO 1381 Security Target

Key	key access method and specification
	<u>(calibration phase)</u>
<u>Pairing key of the motion sensor <math>K_p</math></u>	<u>temporarily reconstructed from Enc (<math>K_m/ K_p</math>) a motion sensor identification key <math>K_{ID}</math> as specified in [16844-3], sec. 7.2, 7.4.3 (calibration phase)</u>
<u>session key between motion sensor and vehicle unit <math>K_{sm}</math></u>	<u>Internally generated and temporary stored during session between the TOE and the motion sensor connected (calibration and operational phases)</u>
<u>session key between tachograph cards and vehicle unit <math>K_{st}</math></u>	<u>Internally generated and temporary stored during session between the TOE and the tachograph card connected (calibration and operational phases)</u>
<u>European public key EUR.PK</u>	<u>Stored during manufacturing of the TOE calibration and operational phases)</u>
<u>equipment private key <math>EQT_i.SK</math></u>	<u>Stored during manufacturing of the TOE (calibration and operational phases)</u>
<u>part of the Master key <math>K_{vu}</math></u>	<u>Stored during manufacturing of the TOE (calibration and operational phases)</u>
<u>security device public key <math>SECDEV.PK</math></u>	<u>Stored during manufacturing of the TOE</u>
<u>transport key software upgrade <math>K_t</math></u>	<u>temporarily decoded from the transmitted data from the management device (at most by the end of the software upgrade)</u>
<u>Individual device key <math>K_{vu}</math></u>	<u>Stored during manufacturing of the TOE</u>

1


## 2 FCS\_CKM.4 Cryptographic key destruction {CSP\_205}

Hierarchical to: -

Dependencies: [FDP\_ITC.1 or FDP\_ITC.2 or FCS\_CKM.1]: see explanation for FCS\_CKM.3 above

**FCS\_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method as specified below that meets the following list of standards:


Key	key destruction method
<u>Part of the Master key <math>K_{wc}</math></u>	<u>delete after use (at most by the end of the calibration phase)</u>

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target				Pages 51 of 106	
		Document key					
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Key	key destruction method
<u>Motion sensor Master key Km</u>	<u>Delete after use use (at most by the end of the calibration phase)</u>
motion sensor identification key $K_{ID}$	delete after use (at most by the end of the calibration phase)
<u>Pairing key of the motion sensor <math>K_p</math></u>	<u>delete after use (at most by the end of the calibration phase)</u>
<u>session key between motion sensor and vehicle unit <math>K_{sm}</math></u>	<u>Delete for replacement (by closing a motion sensor communication session during the pairing process)</u>
<u>session key between tachograph cards and vehicle unit <math>K_{st}</math></u>	<u>Delete for replacement (by closing a card communication session)</u>
<u>European public key EUR.PK</u>	<u>These public keys does not represent any secret and, hence, needn't to be deleted.</u>
<u>equipment private key <math>EQT_j.SK</math></u>	<u>will be loaded into the TOE outside of its operational phase, cf. also OE.Sec Data xx. and must not be destroyed as long as the TOE is operational</u>
<u>part of the Master key <math>Km_{vu}</math></u>	<u>will be loaded into the TOE outside of its operational phase, cf. also OE.Sec Data xx. and must not be destroyed as long as the TOE is operational</u>
<u>Individual device key <math>K_{vu}</math></u>	<u>will be loaded into the TOE outside of its operational phase, cf. also OE.Sec Data xx. and must not be destroyed as long as the TOE is operational</u>
<u>security device public key SECDEV.PK</u>	<u>These public keys does not represent any secret and, hence, needn't to be deleted.</u>
<u>transport key software upgrade <math>K_t</math></u>	<u>Delete after use use (at most by the end of the calibration phase)</u>

**Application Note 11:** The component FCS\_CKM.4 relates to any instantiation of cryptographic keys independent of whether it is of *temporary* or *permanent* nature. In contrast, the component FDP\_RIP.1 concerns in this ST only the temporarily stored instantiations of objects in question. The permanently stored instantiations of  $EQT_j.SK$  and of the part of the Master key  $Km_{vu}$  must not be destroyed as long as the TOE is operational. Making the permanently stored instantiations of  $EQT_j.SK$  and of the part of the Master key  $Km_{vu}$  unavailable at decommissioning the TOE is a matter of the related organisational policy

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				52 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

- 1
- 2 9.1.4.2 FCS\_COP Cryptographic operation
- 3 **FCS\_COP.1/TDES** Cryptographic operation **{CSP\_201}**

Hierarchical to: -  
 Dependencies: [FDP\_ITC.1 or FDP\_ITC.2 or FCS\_CKM.1]: is fulfilled by FCS\_CKM.1  
 FCS\_CKM.4: is fulfilled by FCS\_CKM.4

4 **FCS\_COP.1.1/TDES** The TSF shall perform the cryptographic operations (encryption,  
 5 decryption, Retail-MAC) in accordance with a specified cryptographic algorithm Triple  
 6 DES in CBC and ECB modes and cryptographic key size 112 bits that meet the  
 7 following: [16844-3] for the Motion Sensor and [3821\_IB\_11] for the Tachograph Cards.

- 8 **FCS\_COP.1/RSA** Cryptographic operation **{CSP\_201}**

Hierarchical to: -  
 Dependencies: [FDP\_ITC.1 or FDP\_ITC.2 or FCS\_CKM.1]: not fulfilled, but **justified**  
 It is a matter of RSA decrypting and verifying in the context of CSM\_020 (VU<->TC authentication) and of RSA signing according to CSM\_034 using static keys imported outside of the VU's operational phase (OE.Sec\_Data\_xx).  
 FCS\_CKM.4: is fulfilled by FCS\_CKM.4

9 **FCS\_COP.1.1/RSA** The TSF shall perform the cryptographic operations (decryption, verifying for the  
 10 Tachograph Cards authentication and signing for downloading to external media) in accordance with a  
 11 specified cryptographic algorithm RSA and cryptographic key size 1024 bits that meet the following:  
 12 [3821\_IB\_11] for the Tachograph Cards authentication and [3821\_IB\_11], CSM\_034 for downloading  
 13 to external media, respectively.

14 **Application Note 12:** It is a matter of RSA decrypting and verifying in the context of CSM\_020  
 15 ([3821\_IB\_11] – VU <-> TC authentication) using static keys imported outside the VU's  
 16 operational phase (OE.Sec\_Data\_xx). Due to this fact the dependency FDP\_ITC.1 or  
 17 FDP\_ITC.2 or FCS\_CKM.1 is not applicable to these keys.

- 18 9.1.5 Class FDP User Data Protection


- 19 9.1.5.1 FDP\_ACC Access control policy

**FDP\_ACC.1/FIL** Subset access control **{ACC\_211}**

Hierarchical to: -  
 Dependencies: FDP\_ACF.1: is fulfilled by FDP\_ACF.1/FIL

**FDP\_ACC.1.1/FIL** The TSF shall enforce the File Structure SFP on application and data files structure as required by ACC\_211.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization is prohibited. Offenders may be held liable for payment of damages. All rights created by patent, trademark registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com		2015-02-11		I CVAM TTS LRH		
		Designation DTCO 1381 Security Target				Pages 53 of 106	
		Document key					
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

1 **FDP\_ACC.1/FUN** Subset access control **{ACC\_201}**

Hierarchical to: -  
 Dependencies: FDP\_ACF.1: is fulfilled by FDP\_ACF.1/FUN

2 **FDP\_ACC.1.1/FUN** The TSF shall enforce the SFP FUNCTION on the subjects, objects, and  
 3 operations as referred in

- 4 - operational modes {ACC\_202} and the related restrictions on access rights {ACC\_203},
- 5 - calibration functions {ACC\_206} and time adjustment {ACC\_208},
- 6 - limited manual entry {ACR\_201a},
- 7 - Tachograph Card withdrawal {RLB\_213}
- 8 as required by ACC\_201.

9 **FDP\_ACC.1/DAT** Subset access control **{ACC\_201}**

Hierarchical to: -  
 Dependencies: FDP\_ACF.1: is fulfilled by FDP\_ACF.1/DAT

10 **FDP\_ACC.1.1/DAT** The TSF shall enforce the access control SFP DATA on the subjects, objects, and  
 11 operations as required in:

- 12 - VU identification data: {ACT\_202} (REQ075: structure) and {ACC\_204} (REQ076: once recorded),
- 13 - MS identification data: {ACC\_205} (REQ079: Manufacturing-ID and REQ155: pairing),
- 14 - Calibration Mode Data: {ACC\_207} (REQ097) and {ACC\_209} (REQ100),
- 15 - Security Data: {ACC\_210} (REQ080),
- 16 - MS Audit Records: {AUD\_204}<sup>33</sup>
- 17 as required by ACC\_201.

18 **FDP\_ACC.1/UDE** Subset access control **{ACT\_201, ACT\_203, ACT\_204}**: REQ 109 and 109a


Hierarchical to: -  
 Dependencies: FDP\_ACF.1: is fulfilled by FDP\_ACF.1/UDE

19 **FDP\_ACC.1.1/UDE** The TSF shall enforce the SFP User Data Export on the subjects, objects, and  
 20 operations as required in REQ 109 and 109a.

**FDP\_ACC.1/IS** Subset access control **{ACR\_201, RLB\_205}**

Hierarchical to: -  
 Dependencies: FDP\_ACF.1: is fulfilled by FDP\_ACF.1/IS

<sup>33</sup> These data are generated not by the TOE, but by the Motion Sensor. Hence, they represent - from the point of view of the TOE - just a kind of data to be stored.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				54 of 106	
Document key				Copyright ( C ) Continental AG 2008			
Villingen-Schwenningen (VIL)							

# DTCO 1381 Security Target

1 **FDP\_ACC.1.1/IS** The TSF shall enforce the SFP Input Sources on the subjects, objects, and  
 2 operations as required in {ACR 201, RLB 205}.

3 **FDP\_ACC.1/SW-Upgrade** Subset access control **{RLB 205}**

Hierarchical to: -

Dependencies: FDP\_ACF.1: is fulfilled by FDP\_ACF.1/SW-Upgrade

4 **FDP\_ACC.1.1/SW-Upgrade** The TSF shall enforce the SFP SW-Upgrade on the subjects, objects,  
 5 and operations as required in {RLB 205}.

6 9.1.5.2 FDP\_ACF - Access control functions

7 **FDP\_ACF.1/FIL** Security attribute based access control **{ACC 211}**

Hierarchical to: -

Dependencies: FDP\_ACC.1: is fulfilled by FDP\_ACC.1/FIL

FMT\_MSA.3: is fulfilled by FMT\_MSA.3/FIL

8 **FDP\_ACF.1.1/FIL** The TSF shall enforce the File Structure SFP to objects based on the following: the  
 9 entire files structure of the TOE-application as required by ACC 211.

10 **FDP\_ACF.1.2/FIL** The TSF shall enforce the following rules to determine if an operation among  
 11 controlled subjects and controlled objects is allowed: none.

12 **FDP\_ACF.1.3/FIL** The TSF shall explicitly authorise access of subjects to objects based on the  
 13 following additional rules: none.

14 **FDP\_ACF.1.4/FIL** The TSF shall explicitly deny access of subjects to objects based on the following  
 15 additional rules as required by {ACC 211}.

16 **FDP\_ACF.1/FUN** Security attribute based access control **{ACC 202, ACC 203, ACC 206, ACC 208,**  
 17 **ACR 201a, RLB 213}**

Hierarchical to: -

Dependencies: FDP\_ACC.1: is fulfilled by FDP\_ACC.1/FUN

FMT\_MSA.3: is fulfilled by FMT\_MSA.3/FUN

18 **FDP\_ACF.1.1/FUN** The TSF shall enforce SFP FUNCTION to objects based on the following: the  
 19 subjects, objects, and their attributes as referred in:

20 - operational modes {ACC 202} and the related restrictions on access rights {ACC 203}.


- calibration functions {ACC 206} and time adjustment {ACC 208}

- limited manual entry. {ACR 201a} and

- Tachograph Card withdrawal {RLB 213}.

**FDP\_ACF.1.2/FUN** The TSF shall enforce the following rules to determine if an operation among  
 controlled subjects and controlled objects is allowed: rules in {ACC 202,  
ACC 203, ACC 206, ACC 208, ACR 201a, RLB 213}.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization by the holder of the patent, patent application or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages			
Villingen-Schwenningen (VIL)				55 of 106			
				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

1 **FDP\_ACF.1.3/FUN** The TSF shall explicitly authorise access of subjects to objects based on the  
 2 following additional rules: none.

3 **FDP\_ACF.1.4/FUN** The TSF shall explicitly deny access of subjects to objects based on the following  
 4 additional rules: none.

5 **FDP\_ACF.1/DAT** Security attribute based access control {**ACC\_204, ACC\_205, ACC\_207, ACC\_209,**  
 6 **ACC\_210, ACT\_202, AUD\_204**}

Hierarchical to: -  
 Dependencies: FDP\_ACC.1: is fulfilled by FDP\_ACC.1/DAT  
 FMT\_MSA.3: is fulfilled by FMT\_MSA.3/DAT

7 **FDP\_ACF.1.1/DAT** The TSF shall enforce the SFP DATA to objects based on the following: the  
 8 subjects, objects, and their attributes listed in FDP\_ACC.1/DAT above.

9 **FDP\_ACF.1.2/DAT** The TSF shall enforce the following rules to determine if an operation among  
 10 controlled subjects and controlled objects is allowed: the access rules as required  
 11 by {ACC\_204, ACC\_205, ACC\_207, ACC\_209, ACC\_210, ACT\_202, AUD\_204}.

12 **FDP\_ACF.1.3/DAT** The TSF shall explicitly authorise access of subjects to objects based on the  
 13 following additional rules: none.

14 **FDP\_ACF.1.4/DAT** The TSF shall explicitly deny access of subjects to objects based on the *following*  
 15 *additional rules: none*.

16 **FDP\_ACF.1/UDE** Security attribute based access control {**ACT\_201, ACT\_203, ACT\_204**} (REQ109  
 17 and 109a)

Hierarchical to: -  
 Dependencies: FDP\_ACC.1: is fulfilled by FDP\_ACC.1/UDE  
 FMT\_MSA.3: is fulfilled by FMT\_MSA.3/UDE

18 **FDP\_ACF.1.1/UDE** The TSF shall enforce SFP User Data Export to objects based on the following:  
 19 the subjects, objects, and their attributes as referred in REQ109 and 109a.

20 **FDP\_ACF.1.2/UDE** The TSF shall enforce the following rules to determine if an operation among  
 21 controlled subjects and controlled objects is allowed: rules in REQ109 and 109a.


22 **FDP\_ACF.1.3/UDE** The TSF shall explicitly authorise access of subjects to objects based on the  
 23 following additional rules: none.

24 **FDP\_ACF.1.4/UDE** The TSF shall explicitly deny access of subjects to objects based on the *following*  
 25 *additional rules: none*.

**FDP\_ACF.1/IS** Security attribute based access control {**ACR\_201, RLB\_205**}

Hierarchical to: -  
 Dependencies: FDP\_ACC.1: is fulfilled by FDP\_ACC.1/IS  
 FMT\_MSA.3: is fulfilled by FMT\_MSA.3/IS

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				56 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					



# DTCO 1381 Security Target

1 **FDP\_ACF.1.1/IS** The TSF shall enforce SFP Input Sources to objects based on the following: the  
 2 subjects, objects, and their attributes as referred in {ACR 201, RLB 205}.

3 **FDP\_ACF.1.2/IS** The TSF shall enforce the following rules to determine if an operation among  
 4 controlled subjects and controlled objects is allowed: rules in {ACR 201<sup>34</sup>}.

5 **FDP\_ACF.1.3/IS** The TSF shall explicitly authorise access of subjects to objects based on the  
 6 following additional rules: none.

7 **FDP\_ACF.1.4/IS** The TSF shall explicitly deny access of subjects to objects based on the *following*  
 8 *additional rules: as required by {RLB 205}*.

9 **FDP\_ACF.1/SW-Upgrade** Security attribute based access control **{RLB 205}**

- Hierarchical to: -
- Dependencies: FDP\_ACC.1: is fulfilled by FDP\_ACC.1/Software-Upgrade
- FMT\_MSA.3: is fulfilled by FMT\_MSA.3/Software-lpgrade

10

11 **FDP\_ACF.1.1/SW-Upgrade** The TSF shall enforce SFP SW-Upgrade to objects based on the  
 12 following: the subjects, objects, and their attributes as referred in {RLB 205}.

13 **FDP\_ACF.1.2/SW-Upgrade** The TSF shall enforce the following rules to determine if an operation  
 14 among controlled subjects and controlled objects is allowed: rules as defined by  
 15 FDP\_ITC.2/SW-Upgrade.

16 **FDP\_ACF.1.3/SW-Upgrade** The TSF shall explicitly authorise access of subjects to objects based on  
 17 the following additional rules: none.

18 **FDP\_ACF.1.4/SW-Upgrade** The TSF shall explicitly deny access of subjects to objects based on the  
 19 following additional rule: all data not recognized as an authentic SW-Upgrade.

20 9.1.5.3 FDP\_ETC Export from the TOE

21 **FDP\_ETC.2** Export of user data with security attributes **{ACT\_201, ACT\_203, ACT\_204, ACT\_207,**  
 22 **AUD\_201, DEX\_205, DEX\_208}** (REQ109 and 109a)

- Hierarchical to: -
- Dependencies: [FDP\_ACC.1 or FDP\_IFC.1]: is fulfilled by FDP\_ACC.1/UDE


23 **FDP\_ETC.2.1** The TSF shall enforce the SFP User Data Export when exporting user data, controlled  
 24 under the SFP(s), outside of the TOE.

25 **FDP\_ETC.2.2** The TSF shall export the user data with the user data's associated security attributes.

26 **FDP\_ETC.2.3** The TSF shall ensure that the security attributes, when exported outside the TOE, are  
 27 unambiguously associated with the exported user data.

28 **FDP\_ETC.2.4** The TSF shall enforce the following rules when user data is exported from the TOE:  
 29 REQ110, DEX\_205, DEX\_208.

34 Especially for the MS and the TC

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				57 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					

# DTCO 1381 Security Target

1 9.1.5.4 FDP\_ITC Import from outside of the TOE

2 **FDP\_ITC.1** Import of user data without security attributes **{ACR\_201}**

Hierarchical to: -

Dependencies: [FDP\_ACC.1 or FDP\_IFC.1]: is fulfilled by FDP\_ACC.1/IS  
 FMT\_MSA.3: is fulfilled by FMT\_MSA.3/IS

3 **FDP\_ITC.1.1** The TSF shall enforce the SFP Input Sources when importing user data, controlled  
 4 under the SFP, from outside of the TOE.

5 **FDP\_ITC.1.2** The TSF shall ignore any security attributes associated with the user data when imported  
 6 from outside the TOE.

7 **FDP\_ITC.1.3** The TSF shall enforce the following rules when importing user data controlled under the  
 8 SFP from outside the TOE: as required by {ACR\_201} for recording equipment  
 9 calibration parameters and user's inputs.

10 **FDP\_ITC.2//IS** Import of user data with security attributes **{ACR\_201, DEX\_201, DEX\_202, DEX\_203,**  
 11 **DEX\_204, RLB\_205}**

Hierarchical to: -

Dependencies: [FDP\_ACC.1 or FDP\_IFC.1]: is fulfilled by FDP\_ACC.1/IS  
 [FTP\_ITC.1 or FTP\_TRP.1]: not fulfilled, but **justified**:

Indeed, trusted channels VU<->MS and VU<->TC will be established. Since the component FTP\_ITC.1 represents just a higher abstraction level integrative description of this property and does not define any additional properties comparing to {FDP\_ITC.2//IS + FDP\_ETC.2 + FIA\_UAU.1/TC (and /MS)}, it can be dispensed with this dependency in the current context of the ST.

FPT\_TDC.1: is fulfilled by FPT\_TDC.1//IS

12 **FDP\_ITC.2.1//IS** The TSF shall enforce the SFP Input Sources when importing user data, controlled  
 13 under the SFP, from outside of the TOE.

14 **FDP\_ITC.2.2//IS** The TSF shall use the security attributes associated with the imported user data.


15 **FDP\_ITC.2.3//IS** The TSF shall ensure that the protocol used provides for the unambiguous  
 16 association between the security attributes and the user data received.

17 **FDP\_ITC.2.4//IS** The TSF shall ensure that interpretation of the security attributes of the imported user  
 18 data is as intended by the source of the user data.

**FDP\_ITC.2.5//IS** The TSF shall enforce the following rules when importing user data controlled under  
 the SFP from outside the TOE as required by:

- [16844-3] for the Motion Sensor {ACR\_201, DEX\_201}
- DEX\_202 (audit record and continue to use imported data)
- [3821 IB 11] for the Tachograph Cards {ACR\_201, DEX\_203} - DEX\_204 (audit record and not using of the data).
- RLB\_205 (no executable code from external sources).

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization of the publisher may be held liable for payment of damages. All rights reserved, including registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						58 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

1 **FDP\_ITC.2//SW-Upgrade** Import of user data with security attributes {RLB\_205}

Hierarchical to: -

Dependencies: [FDP\_ACC.1 or FDP\_IFC.1]: is fulfilled by FDP\_ACC.1/Software-Upgrade

[FTP\_ITC.1 or FTP\_TRP.1]: not fulfilled, but **justified**:

Indeed, trusted channel VU<->MD will be established. Since the component FTP\_ITC.1 represents just a higher abstraction level integrative description of this property and does not define any additional properties comparing to {FDP\_ITC.2//Software-Upgrade + FDP\_ETC.2 + FIA\_UAU.1/MDMS}), it can be dispensed with this dependency in the current context of the ST.

FPT\_TDC.1: is fulfilled by FPT\_TDC.1//Software-Upgrade

2 **FDP\_ITC.2.1//SW-Upgrade** The TSF shall enforce the SFP SW-Upgrade when importing user data,  
3 controlled under the SFP, from outside of the TOE.

4 **FDP\_ITC.2.2//SW-Upgrade** The TSF shall use the security attributes associated with the imported  
5 user data.

6 **FDP\_ITC.2.3 //SW-Upgrade** The TSF shall ensure that the protocol used provides for the  
7 unambiguous association between the security attributes and the user data  
8 received.

9 **FDP\_ITC.2.4//SW-Upgrade** The TSF shall ensure that interpretation of the security attributes of the  
10 imported user data is as intended by the source of the user data.

11 **FDP\_ITC.2.5//SW-Upgrade** The TSF shall enforce the following rules when importing user data  
12 controlled under the SFP from outside the TOE: only data recognized as  
13 an authentic SW-Upgrade are allowed to be accepted as executable code:  
14 else they must be rejected.

15 9.1.5.5 FDP\_RIP Residual information protection


16 **FDP\_RIP.1** Subset residual information protection {REU\_201}

Hierarchical to: -

Dependencies: -

17 **FDP\_RIP.1.1** The TSF shall ensure that any previous information content of a **temporarily stored**  
18 resource is made unavailable upon the deallocation of the resource from the following  
19 objects:

Object Reuse for
<u>Part of the Master key <math>K_{m_{WC}}</math> (at most by the end of the calibration phase)</u>
<u>Motion sensor Master key <math>K_m</math> (at most by the end of the calibration phase)</u>
<u>motion sensor identification key <math>K_{ID}</math> (at most by the end of the calibration phase)</u>

Designed by	Date	Department	Sign
winfried.rogenz@continental-corporation.com	2015-02-11	I CVAM TTS LRH	
Released by	2015-02-11	I CVAM TTS LRH	
		Designation DTCO 1381 Security Target	Pages 59 of 106
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008	

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

# DTCO 1381 Security Target

Object Reuse for
<u>Pairing key of the motion sensor <math>K_p</math> (at most by the end of the calibration phase)</u>
<u>session key between motion sensor and vehicle unit <math>K_{sm}</math> (when its temporarily stored value is not in use anymore)</u>
<u>session key between tachograph cards and vehicle unit <math>K_{st}</math> (by closing a card communication session)</u>
<u>equipment private key <math>EQT_j.SK</math> (when its temporarily stored value is not in use anymore)</u>
<u>part of the Master key <math>Km_{vu}</math> (when its temporarily stored value is not in use anymore)</u>
<u>PIN: The verification value of the workshop card PIN temporarily stored in the TOE during its calibration (at most by the end of the calibration phase)</u>
<u>transport key software upgrade <math>Kt</math> (at most by the end of the calibration phase)</u>

1

2 **Application Note 13:** The component FDP\_RIP.1 concerns in this ST only the temporarily stored  
 3 (e.g. in RAM) instantiations of objects in question. In contrast, the component FCS\_CKM.4 relates to  
 4 any instantiation of cryptographic keys independent of whether it is of *temporary* or *permanent* nature.  
 5 Making the permanently stored instantiations of  $EQT_j.SK$  and of the part of the Master key  $Km_{vu}$   
 6 unavailable at decommissioning the TOE is a matter of the related organisational policy.

7 **Application Note 14:** The functional family FDP\_RIP possesses such a general character, so that it  
 8 is applicable not only to user data (as assumed by the class FDP), but also to TSF-data.

9 9.1.5.6 FDP\_SDI Stored data integrity

10 **FDP\_SDI.2** Stored data integrity {ACR\_204, ACR\_205}

Hierarchical to: -

Dependencies: -

11 **FDP\_SDI.2.1** The TSF shall monitor user data stored in the **TOE's data memory** in ~~containers~~  
 12 ~~controlled by the TSF for integrity errors on all objects, based on the following attributes:~~  
 13 ~~user data attributes.~~


14 **FDP\_SDI.2.2** Upon detection of a data integrity error, the TSF shall generate an audit record.

15 **Application Note 15:** The context for the current SFR is built by the related requirements ACR\_204,  
 ACR\_205 (sec. 4.6.3 of 3821\_IB\_10] 'Stored data integrity'). This context gives a clue for  
 interpretation that it is not a matter of temporarily, but of permanently stored user data.<sup>35</sup>

9.1.6 Class FIA Identification and Authentication

9.1.6.1 FIA\_AFL Authentication failures

<sup>35</sup> see definition in glossary

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				60 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					

# DTCO 1381 Security Target

1 **FIA\_AFL.1/MS** Authentication failure handling {**UIA\_206**}

Hierarchical to: -  
 Dependencies: FIA\_UAU.1: is fulfilled by FIA\_UAU.2//MS

2  
 3 **FIA\_AFL.1.1/MS** The TSF shall detect when 2 unsuccessful authentication attempts occur related to  
 4 motion sensor authentication.

5 **FIA\_AFL.1.2/MS** When the defined number of unsuccessful authentication attempts has been  
 6 surpassed, the TSF shall  
 7 generate an audit record of the event,  
 8 warn the user,  
 9 continue to accept and use non secured motion data sent by the motion sensor.

10 **Application Note 16:** The positive integer number expected above shall be  $\leq 20$ , cf. UIA\_206 in  
 11 3821\_IB\_10].

12 **FIA\_AFL.1/TC** Authentication failure handling {**UIA\_214**}

Hierarchical to: -  
 Dependencies: FIA\_UAU.1: is fulfilled by FIA\_UAU.1/TC

13 **FIA\_AFL.1.1/TC** The TSF shall detect when 5 unsuccessful authentication attempts occur related to  
 14 tachograph card authentication.

15 **FIA\_AFL.1.2/TC** When the defined number of unsuccessful authentication attempts has been  
 16 surpassed, the TSF shall  
 17 generate an audit record of the event,  
 18 warn the user,  
 19 assume the user as UNKNOWN and the card as non valid<sup>36</sup> (definition z and  
 20 REQ007).

21 **FIA\_AFL.1/Remote** Authentication failure handling {**UIA\_220**}

Hierarchical to: -  
 Dependencies: FIA\_UAU.1: is fulfilled by FIA\_UAU.1/TC


22 **FIA\_AFL.1.1/Remote** The TSF shall detect when 5 unsuccessful authentication attempts occur related  
 23 to tachograph card authentication.

24 **FIA\_AFL.1.2 /Remote** When the defined number of unsuccessful authentication attempts has been  
 25 surpassed, the TSF shall  
 26 warn the remotely connected company.

## 9.1.6.2 FIA\_ATD User attribute definition

### **FIA\_ATD.1//TC** User attribute definition {**UIA\_208, UIA\_216**}

<sup>36</sup> is commensurate with 'Unknown equipment' in the current PP

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				61 of 106	
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Hierarchical to: -

Dependencies: -

1 **FIA\_ATD.1.1/TC** The TSF shall maintain the following list of security attributes belonging to individual  
 2 users: as defined in {UIA\_208, UIA\_216}.

3 9.1.7 FIA\_UAU User authentication

4 **FIA\_UAU.1/TC** Timing of authentication {UIA\_209, UIA\_217}

Hierarchical to: -

Dependencies: FIA\_UID.1: is fulfilled by FIA\_UID.2/TC

5 **FIA\_UAU.1.1/TC** The TSF shall allow (i) TC identification as required by FIA\_UID.2.1/TC and (ii)  
 6 reading out audit records as required by FAU\_SAR.1 on behalf of the user to be  
 7 performed before the user is authenticated<sup>37</sup>.

8 **FIA\_UAU.1.2/TC** The TSF shall require each user to be successfully authenticated before allowing any  
 9 other TSF-mediated actions on behalf of that user.

10 **FIA\_UAU.1/PIN** Timing of authentication {UIA\_212}

Hierarchical to: -

Dependencies: FIA\_UID.1: is fulfilled by FIA\_UID.2/TC<sup>38</sup>

11 **FIA\_UAU.1.1/PIN** The TSF shall allow (i) TC (Workshop Card) identification as required by  
 12 FIA\_UID.2.1/TC and (ii) reading out audit records as required by FAU\_SAR.1 on  
 13 behalf of the user to be performed before the user is authenticated<sup>39</sup>.

14 **FIA\_UAU.1.2/PIN** The TSF shall require each user to be successfully authenticated before allowing  
 15 any other TSF-mediated actions on behalf of that user.

16 **FIA\_UAU.1/MD** Timing of authentication {UIA\_222}

Hierarchical to: -

Dependencies: FIA\_UID.1: is fulfilled by FIA\_UID.2/TC<sup>40</sup>

17 **FIA\_UAU.1.1/MD** The TSF shall allow MD identification on behalf of the user to be performed before  
 18 the user is authenticated<sup>41</sup>.


<sup>37</sup> According to CSM\_20 in [3821\_IB\_11] the TC identification (certificate exchange) is to perform strictly before the mutual authentication between the VU and the TC.

<sup>38</sup> the PIN-based authentication is applicable for the workshop cards, whose identification is ruled by FIA\_UID.2/TC

<sup>39</sup> According to CSM\_20 in [3821\_IB\_11] the TC identification (certificate exchange) is to perform strictly before the PIN authentication of the Workshop Card.

<sup>40</sup> the PIN-based authentication is applicable for the workshop cards, whose identification is ruled by FIA\_UID.2/TC

<sup>41</sup> According to the respective communication protocol the MD identification (certificate exchange) is to perform strictly before the authentication of the MD.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 62 of 106	
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

---

1 **FIA\_UAU.1.2/MD** The TSF shall require each user to be successfully authenticated before allowing  
 2 any other TSF-mediated actions on behalf of that user.

3 **FIA\_UAU.2//MS** User authentication before any action {UIA\_203}<sup>42</sup>.

Hierarchical to: FIA\_UAU.1

Dependencies: FIA\_UID.1: is fulfilled by FIA\_UID.2/MS

4 **FIA\_UAU.2.1//MS** The TSF shall require each user to be successfully authenticated before allowing  
 5 any other TSF-mediated actions on behalf of that user.

6 **FIA\_UAU.3/MS** Unforgeable authentication {UIA\_205}

Hierarchical to: -

Dependencies: -

7 **FIA\_UAU.3.1/MS** The TSF shall detect and prevent use of authentication data that has been forged by  
 8 any user of the TSF.

9 **FIA\_UAU.3.2/MS** The TSF shall detect and prevent use of authentication data that has been copied  
 10 from any other user of the TSF.

11 **FIA\_UAU.3/TC** Unforgeable authentication {UIA\_213, UIA\_219}

Hierarchical to: -

Dependencies: -

12 **FIA\_UAU.3.1/TC** The TSF shall detect and prevent use of authentication data that has been forged by  
 13 any user of the TSF.

14 **FIA\_UAU.3.2/TC** The TSF shall detect and prevent use of authentication data that has been copied  
 15 from any other user of the TSF.

16 **FIA\_UAU.3/MD** Unforgeable authentication {UIA\_223}

Hierarchical to: -

Dependencies: -

17 **FIA\_UAU.3.1/MD** The TSF shall detect and prevent use of authentication data that has been forged by  
 18 any user of the TSF.


19 **FIA\_UAU.3.2/MD** The TSF shall detect and prevent use of authentication data that has been copied  
 20 from any other user of the TSF.

**FIA\_UAU.5/TC** Multiple authentication mechanisms {UIA\_211, UIA\_218}.

Hierarchical to: -

Dependencies: -

<sup>42</sup> Though MS identification happens before the MS authentication, they will be done within same command (80 or 11); hence, it is also plausible to choose here the functional component FIA\_UAU.2.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 63 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

1 **FIA\_UAU.5.1/TC** The TSF shall provide multiple authentication mechanisms according to CSM 20 in  
 2 [3821\_IB\_11] to support user authentication.

3 **FIA\_UAU.5.2/TC** The TSF shall authenticate any user's claimed identity according to the CSM 20 in  
 4 [3821\_IB\_11].

5 **FIA\_UAU.6/MS** Re-authenticating {**UIA\_204**}.

Hierarchical to: -

Dependencies: -

6 **FIA\_UAU.6.1/MS** The TSF shall re-authenticate the user under the conditions every 30 seconds, in  
 7 power save mode up to 45 minutes.

8 **Application Note 17:** The condition under which re-authentication is required expected above shall be  
 9 more frequently than once per hour, cf. UIA\_204 in 3821\_IB\_10].

10 **FIA\_UAU.6/TC** Re-authenticating {**UIA\_210**}

Hierarchical to: -

Dependencies: -

11 **FIA\_UAU.6.1/TC** The TSF shall re-authenticate the user under the conditions twice a day.

12 **Application Note 18:** The condition under which re-authentication is required expected above shall be  
 13 more frequently than once per day, cf. UIA\_210 in 3821\_IB\_10].

## 14 9.1.7.3 FIA\_UID - User identification

15 **FIA\_UID.2/MS** User identification before any action {**UIA\_201**}.

Hierarchical to: FIA\_UID.1

Dependencies: -

16 **FIA\_UID.2.1/MS** The TSF shall require each user to be successfully identified before allowing any  
 17 other TSF-mediated actions on behalf of that user.

18 **FIA\_UID.2/TC** User identification before any action {**UIA\_207, UIA\_215**}

Hierarchical to: FIA\_UID.1

Dependencies: -

19 **FIA\_UID.2.1/TC** The TSF shall require each user to be successfully identified before allowing any other  
 20 TSF-mediated actions on behalf of that user.


**FIA\_UID.2/MD** User identification before any action {**UIA\_221**}

Hierarchical to: FIA\_UID.1

Dependencies: -

**FIA\_UID.2.1/MD** The TSF shall require each user to be successfully identified before allowing any  
 other TSF-mediated actions on behalf of that user.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization is prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	Date	Department	Sign
winfried.rogenz@continental-corporation.com	2015-02-11	I CVAM TTS LRH	
Released by			
winfried.rogenz@continental-corporation.com	2015-02-11	I CVAM TTS LRH	
		Designation DTCO 1381 Security Target	Pages 64 of 106
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008	



# DTCO 1381 Security Target

1 9.1.8 Class FMT Security Management

2 9.1.8.1 FMT\_MSA - Management of security attributes

3 **FMT\_MSA.1** Management of security attributes {**UIA\_208**}

Hierarchical to: -

Dependencies: [FDP\_ACC.1 or FDP\_IFC.1]: is fulfilled by FDP\_ACC.1/FUN

FMT\_SMR.1: is fulfilled by FMT\_SMR.1//TC

FMT\_SMF.1: is fulfilled by FMT\_SMF.1

4 **FMT\_MSA.1.1** The TSF shall enforce the SFP FUNCTION to restrict the ability to change default the  
5 security attributes User Group, User ID<sup>43</sup> to nobody.

6 **FMT\_MSA.3/FUN** Static attribute initialisation

Hierarchical to: -

Dependencies: FMT\_MSA.1: is fulfilled by FMT\_MSA.1

FMT\_SMR.1: is fulfilled by FMT\_SMR.1//TC

7 **FMT\_MSA.3.1/FUN** The TSF shall enforce the SFP FUNCTION to provide restrictive default values for  
8 security attributes that are used to enforce the SFP.

9 **FMT\_MSA.3.2/FUN** The TSF shall allow nobody to specify alternative initial values to override the  
10 default values when an object or information is created.

11 **FMT\_MSA.3/FIL** Static attribute initialisation

Hierarchical to: -

Dependencies: FMT\_MSA.1: is fulfilled by FMT\_MSA.1

FMT\_SMR.1: is fulfilled by FMT\_SMR.1//TC

12 **FMT\_MSA.3.1/FIL** The TSF shall enforce the File Structure SFP to provide restrictive default values  
13 for security attributes that are used to enforce the SFP.

14 **FMT\_MSA.3.2/FIL** The TSF shall allow nobody to specify alternative initial values to override the  
15 default values when an object or information is created.

16 **FMT\_MSA.3/DAT** Static attribute initialisation


Hierarchical to: -

Dependencies: FMT\_MSA.1: is fulfilled by FMT\_MSA.1

FMT\_SMR.1: is fulfilled by FMT\_SMR.1//TC

**FMT\_MSA.3.1/DAT** The TSF shall enforce the SFP DATA to provide restrictive default values for  
security attributes that are used to enforce the SFP.

<sup>43</sup> see definition of the role 'User' in Table 3 above

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 65 of 106	
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

1 **FMT\_MSA.3.2/DAT** The TSF shall allow nobody to specify alternative initial values to override the  
 2 default values when an object or information is created.

3 **FMT\_MSA.3/UDE** Static attribute initialisation

Hierarchical to: -  
 Dependencies: FMT\_MSA.1: is fulfilled by FMT\_MSA.1  
 FMT\_SMR.1: is fulfilled by FMT\_SMR.1//TC

4 **FMT\_MSA.3.1/UDE** The TSF shall enforce the SFP User Data Export to provide restrictive default  
 5 values for security attributes that are used to enforce the SFP.

6 **FMT\_MSA.3.2/UDE** The TSF shall allow nobody to specify alternative initial values to override the  
 7 default values when an object or information is created.

8 **FMT\_MSA.3/IS** Static attribute initialisation

Hierarchical to: -  
 Dependencies: FMT\_MSA.1: is fulfilled by FMT\_MSA.1  
 FMT\_SMR.1: is fulfilled by FMT\_SMR.1//TC

9 **FMT\_MSA.3.1/IS** The TSF shall enforce the SFP Input Sources to provide restrictive default values for  
 10 security attributes that are used to enforce the SFP.

11 **FMT\_MSA.3.2/IS** The TSF shall allow nobody to specify alternative initial values to override the default  
 12 values when an object or information is created.

13 **FMT\_MSA.3/SW-Upgrade** Static attribute initialisation

Hierarchical to: -  
 Dependencies: FMT\_MSA.1: is fulfilled by FMT\_MSA.1  
 FMT\_SMR.1: is fulfilled by FMT\_SMR.1//TC

14 **FMT\_MSA.3.1/SW-Upgrade** The TSF shall enforce the SFP SW-Upgrade to provide restrictive default  
 15 values for security attributes that are used to enforce the SFP.

16 **FMT\_MSA.3.2/SW-Upgrade** The TSF shall allow nobody to specify alternative initial values to override  
 17 the default values when an object or information is created.


18 9.1.8.2 FMT\_MOF - Management of functions in TSF

**FMT\_MOF.1** Management of security functions behaviour **{RLB\_201}**

Hierarchical to: -  
 Dependencies: FMT\_SMR.1: is fulfilled by FMT\_SMR.1//TC  
 FMT\_SMF.1: is fulfilled by FMT\_SMF.1

**FMT\_MOF.1.1** The TSF shall restrict the ability to enable the functions specified in {RLB\_201} to  
nobody.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization is prohibited. Offenders will be held liable for payment of damages. All rights reserved. This document is a registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				66 of 106	
Document key		Villingen-Schwenningen (VIL)					
Copyright ( C ) Continental AG 2008							

# DTCO 1381 Security Target

1 9.1.8.3 Specification of Management Functions (FMT\_SMF)

2 **FMT\_SMF.1** Specification of Management Functions {UIA\_208}

Hierarchical to: -

Dependencies: -

3 **FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions: all  
 4 operations being allowed only in the calibration mode mode as specified in REQ 010.

5 **FMT\_SMR.1//TC** Security roles {UIA\_208}

Hierarchical to: -

Dependencies: FIA\_UID.1: is fulfilled by FIA\_UID.2/TC

6 **FMT\_SMR.1.1//TC** The TSF shall maintain the roles as defined in {UIA\_208} as User Groups.

7 - DRIVER (driver card).

8 - CONTROLLER (control card).

9 - WORKSHOP (workshop card).

10 - COMPANY (company card).

11 - UNKNOWN (no card inserted).

12 - Motion Sensor

13 - Unknown equipment

14 **FMT\_SMR.1.2//TC** The TSF shall be able to associate users with roles.

15 9.1.9 Class FPR Privacy (FPR)

16 9.1.9.1 FPR\_UNO - Unobservability

17 **FPR\_UNO.1** Unobservability {RLB\_204 for leaked data}

Hierarchical to: -

Dependencies: -


18 **FPR\_UNO.1.1** The TSF shall ensure that all users are unable to observe the **cryptographic**  
 19 operations as required by FCS\_COP.1/TDES and FCS\_COP.1/RSA on cryptographic  
 20 keys being to keep secret (as listed in FCS\_CKM.3 excepting EUR.PK) by the TSF.

**Application Note 19:** To observe the cryptographic operations' means here 'using any TOE external interface in order to gain the values of cryptographic keys being to keep secret'.

9.1.10 Protection of the TSF (FPT)

9.1.10.2 FPT\_FLS - Fail secure

**FPT\_FLS.1** Failure with preservation of secure state.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 67 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorisation is prohibited. Copyrights will be held liable for payment of damages. All rights of research, patent grant or registration of a utility model or design patent are reserved.

# DTCO 1381 Security Target

Hierarchical to: -

Dependencies: -

1 **FPT\_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur: as  
 2 specified in {RLB\_203, RLB\_210, RLB\_211}.

3 9.1.10.3 FPT\_PHP - TSF physical protection

4 **FPT\_PHP.1//Seal** Passive detection of physical attack {RLB\_206}

5 Hierarchical to: -

6 Dependencies: -

7 **FPT\_PHP.1.1//Seal** The TSF shall provide unambiguous detection of physical tampering that might  
 8 compromise the TSF.

9 **FPT\_PHP.1.2//Seal** The TSF shall provide the capability to determine whether physical tampering with  
 10 the TSF's devices or TSF's elements has occurred.

11 **FPT\_PHP.2//Power\_Deviation** Notification of physical attack {RLB\_209}

Hierarchical to: FPT\_PHP.1

Dependencies: FMT\_MOF.1: not fulfilled, but **justified:**

It is a matter of RLB\_209: this function (detection of deviation)  
 must not be deactivated by anybody. But FMT\_MOF.1 is  
 formulated in a not applicable way for RLB\_209

12 **FPT\_PHP.2.1//Power\_Deviation** The TSF shall provide unambiguous detection of physical tampering  
 13 that might compromise the TSF.

14 **FPT\_PHP.2.2//Power\_Deviation** The TSF shall provide the capability to determine whether physical  
 15 tampering with the TSF's devices or TSF's elements has occurred.

16 **FPT\_PHP.2.3//Power\_Deviation** For the devices/elements for which active detection is required in  
 17 {RLB\_209}, the TSF shall monitor the devices and elements and  
 18 notify the user and audit record generation when physical tampering  
 19 with the TSF's devices or TSF's elements has occurred.

20 **Application Note 20:** Is a matter of RLB\_209: this function (detection of power deviation) must not be  
 21 deactivated by anybody. But FMT\_MOF.1 is formulated in a wrong way for RLB\_209.  
 22 Due to this fact the dependency FMT\_MOF.1 is not applicable.


23 **FPT\_PHP.3** Resistance to physical attack {RLB\_204 for stored data}

Hierarchical to: -

Dependencies: -

**FPT\_PHP.3.1** The TSF shall resist physical tampering attacks to the TOE security enforcing part of the  
software in the field after the TOE activation by responding automatically such that the  
 SFRs are always enforced.

9.1.10.4 FPT\_STM - Time stamps

Designed by	Date	Department	Sign
winfried.rogenz@continental-corporation.com	2015-02-11	I CVAM TTS LRH	
Released by			
winfried.rogenz@continental-corporation.com	2015-02-11	I CVAM TTS LRH	
		Designation DTCO 1381 Security Target	Pages 68 of 106
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008	

# DTCO 1381 Security Target

1 **FPT\_STM.1** Reliable time stamps {ACR\_201}

Hierarchical to: -  
 Dependencies: -

2 **FPT\_STM.1.1** The TSF shall be able to provide reliable time stamps.

3 **Application Note 21:** This requirement is the matter of the VU's real time clock.

4 9.1.10.5 FPT\_TDC – Inter-TSF TSF Data Consistency

5 **FPT\_TDC.1//IS** Inter-TSF basic TSF data consistency {ACR\_201}

Hierarchical to: -  
 Dependencies: -

6 **FPT\_TDC.1.1//IS** The TSF shall provide the capability to consistently interpret secure messaging  
 7 attributes as defined by [16844-3] for the Motion Sensor and by [3821 IB 11] for  
 8 the Tachograph Cards when shared between the TSF and another trusted IT product.

9  
 10 **FPT\_TDC.1.2//IS** The TSF shall use the interpretation rules (communication protocols) as defined by  
 11 [16844-3] for the Motion Sensor and by [3821 IB 11] for the Tachograph Cards  
 12 when interpreting the TSF data from another trusted IT product.

13 **FPT\_TDC.1//SW-Upgrade** Inter-TSF basic TSF data consistency {RLB\_205}

Hierarchical to: -  
 Dependencies: -

14 **FPT\_TDC.1.1//SW-Upgrade** The TSF shall provide the capability to consistently interpret secure  
 15 attributes as defined by the proprietary specification for the SW-Upgrade  
 16 by the TOE developer when shared between the TSF and another trusted  
 17 IT product.

18 **FPT\_TDC.1.2//SW-Upgrade** The TSF shall use the interpretation rules (communication protocols) as  
 19 defined by the proprietary specification for the SW-Upgrade by the TOE  
 20 developer when interpreting the TSF data from another trusted IT product.


21 **Application Note 22:** Trusted IT product in this case is a special device of the SW-Upgrade issuer  
 22 preparing the new software for distribution.

9.1.10.6 FPT\_TST - TSF self test

**FPT\_TST.1** TSF testing {RLB\_202}

Hierarchical to: -  
 Dependencies: -

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 69 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

- 1 **FPT\_TST.1.1** The TSF shall run a suite of self tests during initial start-up, periodically during normal
- 2 operation to demonstrate the **integrity of security data and the integrity of stored executable code**
- 3 **(if not in ROM).**
- 4 **FPT\_TST.1.2** The TSF shall verify the integrity of security data .
- 5 **FPT\_TST.1.3** The TSF shall verify the integrity of stored executable code.

## 9.1.11 Resource Utilisation (FRU)

### 9.1.11.7 FRU\_PRS - Priority of service

#### FRU\_PRS.1 Limited priority of service {RLB\_212}

Hierarchical to: -

Dependencies: -

9 **FRU\_PRS.1.1** The TSF shall assign a priority to each subject in the TSF.

10 **FRU\_PRS.1.2** The TSF shall ensure that each access to controlled resources shall be mediated on the

11 basis of the subjects assigned priority.

12 **Application Note 23:** The current assignment is to consider in the context of RLB\_212 (sec. 4.7.6 of

13 3821\_IB\_10] 'Data availability'). Controlled resources in this context may be 'functions and data

14 covered by the current set of SFRs'.

## 9.2 Security assurance requirements

16 The European Regulation [3821\_IB] requires for a vehicle unit the assurance level ITSEC E3, high

17 3821\_IB\_10] as specified in 3821\_IB\_10], chap. 6 and 7.

18 [JIL] defines an assurance package called E3hAP declaring assurance equivalence between the

19 assurance level E3 of an ITSEC certification and the assurance level of the package E3hAP within a

20 Common Criteria (ver. 2.1) certification (in conjunction with the Digital Tachograph System).

21 The current official CCMB version of Common Criteria is Version 3.1, Revision 4. This version defines

22 in its part 3 assurance requirements components partially differing from the respective requirements of

23 CC v2.x.


24 The CC community acts on the presumption that the assurance components of CCv3.1 and

25 CCv2.x are equivalent to each other. Due to this fact, the author of the PP compiled and defined an

26 appropriate assurance package **E3hCC31\_AP** as shown below (validity of this proposal is confined to

27 the Digital Tachograph System).

Assurance Classes	Assurance Family	E3hCC31_AP (based on EAL4)
Development	ADV_ARC	1
	ADV_FSP	4

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages			
Villingen-Schwenningen (VIL)				70 of 106			
				Copyright ( C ) Continental AG 2008			

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


# DTCO 1381 Security Target

Assurance Classes	Assurance Family	E3hCC31_AP (based on EAL4)
	ADV_IMP	1
	ADV_INT	-
	ADV_TDS	3
	ADV_SPM	-
Guidance Documents	AGD_OPE	1
	AGD_PRE	1
Life Cycle Support	ALC_CMC	4
	ALC_CMS	4
	ALC_DVS	1
	ALC_TAT	1
	ALC_DEL	1
	ALC_FLR	-
	ALC_LCD	1
Security Target evaluation	ASE	standard approach for EAL4
Tests	ATE_COV	2
	ATE_DPT	2
	STE_FUN	1
	ATE_IND	2
AVA Vulnerability Assessment	AVA_VAN	5

1 **Application Note 24:** The assurance package E3hCC31\_AP represents the standard assurance  
 2 package EAL4 augmented by the assurance components ATE\_DPT.2 and  
 3 AVA\_VAN.5.  
 4

5 **Application Note 25:** The requirement RLB\_215 is covered by ADV\_ARC (security domain separa-  
 tion); the requirement RLB\_204 is partially covered by ADV\_ARC (self-protec-  
 tion).

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation		DTCO 1381 Security Target			
		Document key				Pages 71 of 106	
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			


# DTCO 1381 Security Target

## 1 9.3 Security requirements rationale

### 2 9.3.1 Security functional requirements rationale

3 The following table provides an overview for security functional requirements coverage also giving an  
 4 evidence for *sufficiency* and *necessity* of the SFRs chosen.  
 5

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
<b>FAU_GEN.1</b>	Audit data generation		x	x								
<b>FAU_SAR.1</b>	Audit review		x	x								
<b>FAU_STG.1</b>	Protected audit trail storage		x	x		X						
<b>FAU_STG.4</b>	Prevention of audit data loss		x	x								
<b>FCO_NRO.1</b>	Selective proof of origin						x			x		
<b>FCS_CKM.1</b>	Cryptographic key generation									x		x
<b>FCS_CKM.2</b>	Cryptographic key distribution									x		
<b>FCS_CKM.3</b>	Cryptographic key access									x		x
<b>FCS_CKM.4</b>	Cryptographic key destruction									x		x
<b>FCS_COP.1/TDES</b>	Cryptographic operation									x		x
<b>FCS_COP.1/RSA</b>	Cryptographic operation									x		x
<b>FDP_ACC.1/FIL</b>	Subset access control	x										
<b>FDP_ACC.1/FUN</b>	Subset access control	x						x	x	x	x	
<b>FDP_ACC.1/DAT</b>	Subset access control	x										

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008				72 of 106	


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.



# DTCO 1381 Security Target

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
<b>FDP_ACC.1/UDE</b>	Subset access control	x										
<b>FDP_ACC.1/IS</b>	Subset access control	x						x	x			
<b>FDP_ACC.1/SW-Upgrade</b>	Subset access control	x						x	x		x	x
<b>FDP_ACF.1/FIL</b>	Security attribute based access control	x										
<b>FDP_ACF.1/FUN</b>	Security attribute based access control	x						x	x	x	x	
<b>FDP_ACF.1/DAT</b>	Security attribute based access control	x										
<b>FDP_ACF.1/UDE</b>	Security attribute based access control	x										
<b>FDP_ACF.1/IS</b>	Security attribute based access control	x						x	x			
<b>FDP_ACF.1/SW-Upgrade</b>	Security attribute based access control	x						x	x		x	x
<b>FDP_ETC.2</b>	Export of user data with security attributes		x			x	x			X		
<b>FDP_ITC.1</b>	Import of user data without security attributes							x	x			
<b>FDP_ITC.2/IS</b>	Import of user data with security attributes							x	x	X		
<b>FDP_ITC.2/SW-Upgrade</b>	Import of user data with security attributes							x	x		x	x
<b>FDP_RIP.1</b>	Subset residual information protection	x						x	x			


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 73 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					

# DTCO 1381 Security Target

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
<b>FDP_SDI.2</b>	Stored data integrity monitoring and action			x		x	x		x			
<b>FIA_AFL.1/MS</b>	Authentication failure handling			x	x				x			
<b>FIA_AFL.1/TC</b>	Authentication failure handling			x	x							
<b>FIA_AFL.1/Remote</b>	Authentication failure handling			x	x							
<b>FIA_ATD.1/TC</b>	User attribute definition			x						x		
<b>FIA_UAU.1/TC</b>	Timing of authentication				x					x		
<b>FIA_UAU.1/PIN</b>	Timing of authentication				x							
<b>FIA_UAU.1/MD</b>	Timing of authentication				x							
<b>FIA_UAU.2/MS</b>	User authentication before any action				x					X		
<b>FIA_UAU.3/MS</b>	Unforgeable authentication				x							
<b>FIA_UAU.3/TC</b>	Unforgeable authentication				x							
<b>FIA_UAU.3/MD</b>	Unforgeable authentication				x							
<b>FIA_UAU.5/TC</b>	Multiple authentication mechanisms	x			x					x		
<b>FIA_UAU.6/MS</b>	Re-authenticating				x					x		
<b>FIA_UAU.6/TC</b>	Re-authenticating				x					x		
<b>FIA_UID.2/MS</b>	User identification before any action	x	x	x	x					x		
<b>FIA_UID.2/TC</b>	User identification before any action	x	x	x	x					x		


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						74 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008					

# DTCO 1381 Security Target

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
<b>FIA_UID.2/MD</b>	Any action	x	x	x	x							
<b>FMT_MSA.1</b>	Management of security attributes	x								X		
<b>FMT_MSA.3/FUN</b>	Static attribute initialisation	x						x	x	X	x	
<b>FMT_MSA.3/FIL</b>	Static attribute initialisation	x										
<b>FMT_MSA.3/DAT</b>	Static attribute initialisation	x										
<b>FMT_MSA.3/IS</b>	Static attribute initialisation	x						x	x			
<b>FMT_MSA.3/UDE</b>	Static attribute initialisation	x										
<b>FMT_MSA.3/SW_Upgrade</b>	Static attribute initialisation	x						x	x		x	x
<b>FMT_MOF.1</b>	Management of security functions	x							x			
<b>FMT_SMF.1</b>	Specification of Management Functions	x								x		
<b>FMT_SMR.1/TC</b>	Security roles	x								x		
<b>FPR_UNO.1</b>	Unobservability						x	x	x		x	
<b>FPT_FLS.1</b>	Failure with preservation of secure state.			x					x			
<b>FPT_PHP.1//Seal</b>	Passive detection of physical attack			x			x		x			
<b>FPT_PHP.2/Power_Deviation</b>	Notification of physical attack								x			
<b>FPT_PHP.3</b>	Resistance to physical attack						x	x	X		x	
<b>FPT_STM.1</b>	Reliable time stamps		x	x				X	x			

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008				75 of 106	

# DTCO 1381 Security Target

		Security objectives										
		O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	O.Software_Analysis	O.Software_Upgrade
<b>FPT_TDC.1/IS</b>	Inter-TSF basic TSF data consistency							x	x			
<b>FPT_TDC.1/SW-Upgrade</b>	Inter-TSF basic TSF data consistency						x	x	x		x	x
<b>FPT_TST.1</b>	TSF testing			x					x			
<b>FRU_PRS.1</b>	Limited priority of service								x			

1

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008				76 of 106	

# DTCO 1381 Security Target

- 1 A detailed justification required for *suitability* of the security functional requirements to achieve the
- 2 security objectives is given below.
- 3

security objectives	Security functional requirement
O.Access	<b>FDP_ACC.1/FIL</b> File structure SFP on application and data files structure
	<b>FDP_ACC.1/FUN</b> SFP FUNCTION on the functions of the TOE
	<b>FDP_ACC.1/DAT</b> SFP DATA on user data of the TOE
	<b>FDP_ACC.1/UDE</b> SFP User_Data_Export for the export of user data
	<b>FDP_ACC.1/IS</b> SFP Input Sources to ensure the right input sources
	<b>FDP_ACC.1/SW-Upgrade</b> SFP SW-Upgrade for the upgrade of the software in the TOE
	<b>FDP_ACF.1/FIL</b> Entire files structure of the TOE-application
	<b>FDP_ACF.1/FUN</b> Defines security attributes for SFP FUNCTION according to the modes of operation
	<b>FDP_ACF.1/DAT</b> Defines security attributes for SFP DATA on user
	<b>FDP_ACF.1/UDE</b> Defines security attributes for SFP User_Data_Export
	<b>FDP_ACF.1/IS</b> Defines security attributes for SFP Input Sources.
	<b>FDP_ACF.1/SW-Upgrade</b> Defines security attributes for SFP SW-Upgrade
	<b>FDP_RIP.1</b> Any previous information content of a resource is made unavailable upon the deallocation of the resource
	<b>FIA_UAU.5/TC</b> Multiple authentication mechanisms according to CSM_20 in [3821_IB_11] to support user authentication.
	<b>FIA_UID.2/MS</b> A motion sensor is successfully identified before allowing any other action
<b>FIA_UID.2/TC</b> A tachograph card is successfully identified before allowing any other action	
<b>FIA_UID.2/MD</b> A management device is successfully identified before allowing any other action	
<b>FMT_MSA.1</b> Provides the SFP FUNCTION to restrict the ability to change default the security attributes User Group, User ID to nobody.	


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com		2015-02-11		I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						77 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


security objectives	Security functional requirement	
	<b>FMT_MSA.3/FUN</b>	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FMT_MSA.3/FIL</b>	Provides the File_Structure SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FMT_MSA.3/DAT</b>	Provides the SFP DATA to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FMT_MSA.3/IS</b>	Provides the SFP Input Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FMT_MSA.3/UDE</b>	Provides the SFP User Data Export to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FMT_MSA.3/SW-Upgrade</b>	Provides the SFP SW_Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FMT_MOF.1</b>	Restrict the ability to enable the test functions specified in {RLB_201} to nobody, and, thus prevents an unintended access to data in the operational phase.
	<b>FMT_SMF.1</b>	Performing all operations being allowed only in the calibration mode.
	<b>FMT_SMR.1/TC</b>	Maintain the roles as defined in {UIA_208} as User Groups.
O.Accountability	<b>FAU_GEN.1</b>	Generates correct audit records

Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
	Document key	Pages 78 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008	

# DTCO 1381 Security Target

security objectives	Security functional requirement	
	<b>FAU_SAR.1</b>	Allows users to read accountability audit records
	<b>FAU_STG.1</b>	Protect the stored audit records from unauthorised deletion
	<b>FAU_STG.4</b>	Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)
	<b>FDP_ETC.2</b>	Provides export of user data with security attributes using the SFP User_Data_Export
	<b>FIA_UID.2/MS</b>	A motion sensor is successfully identified before allowing any other action
	<b>FIA_UID.2/TC</b>	A tachograph card is successfully identified before allowing any other action
	<b>FIA_UID.2/MD</b>	A management device is successfully identified before allowing any other action
	<b>FPT_STM.1</b>	Provides accurate time
O.Audit	<b>FAU_GEN.1</b>	Generates correct audit records
	<b>FAU_SAR.1</b>	Allows users to read accountability audit records
	<b>FAU_STG.1</b>	Protect the stored audit records from unauthorised deletion.
	<b>FAU_STG.4</b>	Prevent loss of audit data loss (overwrite the oldest stored audit records and behave according to REQ 105b if the audit trail is full.)
	<b>FDP_SDI.2</b>	monitors user data stored for integrity error
	<b>FIA_AFL.1/MS</b>	Provides authentication failure events for the motion sensor
	<b>FIA_AFL.1/TC</b>	Provides authentication failure events for the tachograph cards
	<b>FIA_AFL.1/Remote</b>	Provides authentication failure events for the remotely connected company
	<b>FIA_ATD.1/TC</b>	Defines user attributes for tachograph cards
	<b>FIA_UID.2/MS</b>	A motion sensor is successfully identified before allowing any other action
	<b>FIA_UID.2/TC</b>	A tachograph card is successfully identified before allowing any other action
	<b>FIA_UID.2/MD</b>	A management device is successfully identified before allowing any other action
	<b>FPT_FLS.1</b>	Preserves a secure state when the following types of failures occur: as specified in {RLB_203,


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
	Document key	Pages 79 of 106	
Villingen-Schwenningen (VL)	Copyright ( C ) Continental AG 2008		

# DTCO 1381 Security Target

security objectives	Security functional requirement	
	<b>FPT_PHP.1//Seal</b> <b>FPT_STM.1</b>	RLB_210, RLB_211} Passive detection of physical attack Provides accurate time
O.Authentication	<b>FPT_TST.1</b> <b>FIA_AFL.1/MS</b> <b>FIA_AFL.1/TC</b> <b>FIA_AFL.1/Remote</b> <b>FIA_UAU.1/TC</b> <b>FIA_UAU.1/PIN</b> <b>FIA_UAU.1/MD</b> <b>FIA_UAU.2/MS</b> <b>FIA_UAU.3/MS</b> <b>FIA_UAU.3/TC</b> <b>FIA_UAU.3/MD</b> <b>FIA_UAU.5/TC</b> <b>FIA_UAU.6/MS</b> <b>FIA_UAU.6/TC</b> <b>FIA_UID.2/MS</b> <b>FIA_UID.2/TC</b> <b>FIA_UID.2/MD</b> <b>FAU_STG.1</b> <b>FDP_ETC.2</b>	Detects integrity failure events for security data and stored executable code Detects and records authentication failure events for the motion sensor Detects and records authentication failure events for the tachograph cards Detects and records authentication failure events for the remotely connected company Allows TC identification before authentication Allows TC (Workshop Card) identification before authentication Allows MD identification before authentication Motion sensor has to be successfully authenticated before allowing any action Provides unforgeable authentication for the motion sensor Provides unforgeable authentication for the tachograph cards Provides unforgeable authentication for the management device Multiple authentication mechanisms according to CSM_20 in [3821_IB_11] to support user authentication. Periodically re-authenticate the motion sensor Periodically re-authenticate the tachograph cards A motion sensor is successfully identified before allowing any other action A tachograph card is successfully identified before allowing any other action A management device is successfully identified before allowing any other action. Protect the stored audit records from unauthorised deletion Provides export of user data with security attributes using the access control SFP
O.Integrity		

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
	Document key	Pages 80 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008	



# DTCO 1381 Security Target

security objectives	Security functional requirement	
	<b>FDP_SDI.2</b>	User_Data_Export monitors user data stored for integrity error
O.Output	<b>FCO_NRO.1</b>  <b>FDP_ETC.2</b>  <b>FDP_SDI.2</b>  <b>FPR_UNO.1</b>  <b>FPT_PHP.1//Seal</b>  <b>FPT_PHP.3</b>  <b>FPT_TDC.1//SW-Upgrade</b>	Generates an evidence of origin for the data to be downloaded to external media.  Provides export of user data with security attributes using the access control SFP User_Data_Export  monitors user data stored for integrity error  Ensures unobservability of secrets  Passive detection of physical attack  Ensures resistance to physical attack to the TOE software in the field after the TOE activation  Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer
O.Processing	<b>FDP_ACC.1/FUN</b>  <b>FDP_ACC.1/IS</b>  <b>FDP_ACC.1//SW-Upgrade</b>  <b>FDP_ACF.1/FUN</b>  <b>FDP_ACF.1/IS</b>  <b>FDP_ACF.1//SW-Upgrade</b>  <b>FDP_ITC.1</b>  <b>FDP_ITC.2/IS</b>  <b>FDP_ITC.2//SW-Upgrade</b>	Defines security attributes for SFP FUNCTION according to the modes of operation  SFP Input Sources to ensure the right input sources  Defines security attributes for SFP SW-Upgrade  Defines security attributes for SFP FUNCTION according to the modes of operation  Defines security attributes for SFP User_Data_Export  Defines security attributes for SFP SW-Upgrade  Provides import of user data from outside of the TOE using the <i>SFP Input Sources</i>  Provides import of user data from outside of the TOE using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards  Provides import of user data, from outside of the TOE using the SFP SW-Upgrade. : Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected.


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
	Document key	Pages 81 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008	

# DTCO 1381 Security Target

security objectives	Security functional requirement	
	<b>FDP_RIP.1</b>	Any previous information content of a resource is made unavailable upon the deallocation of the resource
	<b>FMT_MSA.3/FUN</b>	Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FMT_MSA.3/IS</b>	Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FMT_MSA.3/SW-Upgrade</b>	Provides the SFP SW_Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.
	<b>FPR_UNO.1</b>	Ensures unobservability of secrets
	<b>FPT_PHP.3</b>	Ensures Resistance to physical attack to the TOE. 2.1 software in the field after the TOE activation
	<b>FPT_STM.1</b>	Provides accurate time
	<b>FPT_TDC.1/IS</b>	Provides the capability to consistently interpret secure messaging attributes as defined by [16844-3] for the Motion Sensor and by[3821_IB_11] for the Tachograph Cards.
	<b>FPT_TDC.1/SW-Upgrade</b>	Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer
O.Reliability	<b>FDP_ACC.1/FUN</b>	Defines security attributes for SFP FUNCTION according to the modes of operation
	<b>FDP_ACC.1/IS</b>	SFP Input Sources to ensure the right input sources
	<b>FDP_ACC.1/SW-Upgrade</b>	Defines security attributes for SFP SW-Upgrade
	<b>FDP_ACF.1/FUN</b>	Defines security attributes for SFP FUNCTION according to the modes of operation
	<b>FDP_ACF.1/IS</b>	Defines security attributes for SFP



Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
	Document key	Pages 82 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008	

# DTCO 1381 Security Target

security objectives	Security functional requirement
	<p>User_Data_Export</p> <p><b>FDP_ACF.1/SW-Upgrade</b> Defines security attributes for SFP SW-Upgrade</p> <p><b>FDP_ITC.1</b> Provides import of user data from outside of the TOE using the <i>SFP Input Sources</i></p> <p><b>FDP_ITC.2/IS</b> Provides import of user data from outside of the TOE, using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards</p> <p><b>FDP_ITC.2/SW-Upgrade</b> Provides import of user data, from outside of the TOE using the SFP SW-Upgrade. Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected.</p> <p><b>FDP_RIP.1</b> Any previous information content of a resource is made unavailable upon the deallocation of the resource</p> <p><b>FDP_SDI.2</b> monitors user data stored for integrity error</p> <p><b>FIA_AFL.1/MS</b> Provides authentication failure events for the motion sensor</p> <p><b>FIA_AFL.1/TC</b> Provides authentication failure events for the tachograph cards</p> <p><b>FMT_MOF.1</b> Restrict the ability to enable the functions specified in <b>{RLB_201}</b> to nobody.</p> <p><b>FMT_MSA.3/FUN</b> Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p><b>FMT_MSA.3/IS</b> Provides the SFP Input_Sources to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p><b>FMT_MSA.3/SW-Upgrade</b> Provides the SFP SW_Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p>


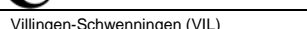
Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
		Document key	Pages 83 of 106
Villingen-Schwenningen (VIL)	Copyright (C) Continental AG 2008		

# DTCO 1381 Security Target

security objectives	Security functional requirement	
	<p><b>FPR_UNO.1</b></p> <p><b>FPT_FLS.1</b></p> <p><b>FPT_PHP.1//Seal</b></p> <p><b>FPT_PHP.2/Power_Deviation</b></p> <p><b>FPT_PHP.3</b></p> <p><b>FPT_STM.1</b></p> <p><b>FPT_TDC.1/IS</b></p> <p><b>FPT_TDC.1/SW-Upgrade</b></p> <p><b>FPT_TST.1</b></p> <p><b>FRU_PRS.1</b></p>	<p>Ensures unobservability of secrets</p> <p>Preserves a secure state when the following types of failures occur: as specified in {RLB_203, RLB_210, RLB_211}</p> <p>Passive detection of physical attack</p> <p>Detection of physical tampering (Power_Deviation) and generation of an audit record</p> <p>Ensures Resistance to physical attack to the TOE software in the field after the TOE activation</p> <p>Provides accurate time</p> <p>Provides the capability to consistently interpret secure messaging attributes as defined by [16844-3] for the Motion Sensor and by[3821_IB_11] for the Tachograph Cards.</p> <p>Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer</p> <p>Detects integrity failure events for security data and stored executable code</p> <p>Ensures that resources will be available when needed</p>
O.Secured_Data_Exchange	<p><b>FCO_NRO.1</b></p> <p><b>FCS_CKM.1</b></p> <p><b>FCS_CKM.2</b></p> <p><b>FCS_CKM.3</b></p> <p><b>FCS_CKM.4</b></p> <p><b>FCS_COP.1/TDES</b></p> <p><b>FCS_COP.1/RSA</b></p> <p><b>FDP_ACC.1/FUN</b></p> <p><b>FDP_ACF.1/FUN</b></p>	<p>Generates an evidence of origin for the data to be downloaded to external media.</p> <p>Generates of session keys for the motion sensor and the tachograph cards</p> <p>Controls distribution of cryptographic keys in accordance with a specified cryptographic key distribution method as specified in the table below that meets the following list of standards.</p> <p>Controls cryptographic key access and storage in the TOE</p> <p>Destroys cryptographic keys in the TOE</p> <p>Provides the cryptographic operation TDES</p> <p>Provides the cryptographic operation RSA</p> <p>Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>Defines security attributes for SFP FUNCTION</p>


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	
	Designation <b>DTCO 1381 Security Target</b>	Pages <b>84 of 106</b>				
		Document key Copyright (C) Continental AG 2008				

# DTCO 1381 Security Target

security objectives	Security functional requirement	
	<b>FDP_ETC.2</b>	according to the modes of operation Provides export of user data with security attributes using the SFP User_Data_Export
	<b>FDP_ITC.2/IS</b>  <b>FIA_ATD.1/TC</b> <b>FIA_UAU.1/TC</b> <b>FIA_UAU.2/MS</b>  <b>FIA_UAU.5/TC</b>  <b>FIA_UAU.6/MS</b> <b>FIA_UAU.6/TC</b> <b>FIA_UID.2/MS</b>  <b>FIA_UID.2/TC</b>  <b>FMT_MSA.1</b>  <b>FMT_MSA.3/FUN</b>  <b>FMT_SMF.1</b>  <b>FMT_SMR.1/TC</b>	Provides import of user data from outside of the TOE using the security attributes associated with the imported user data for the Motion Sensor and for the Tachograph Cards  Defines user attributes for tachograph cards Allows TC identification before authentication Motion sensor has to be successfully authenticated before allowing any action Multiple authentication mechanisms according to CSM_20 in [3821_IB_11] to support user authentication. Periodically re-authenticate the motion sensor Periodically re-authenticate the tachograph cards A motion sensor is successfully identified before allowing any other action A tachograph card is successfully identified before allowing any other action Provides the SFP FUNCTION to restrict the ability to change default the security attributes User Group, User ID to nobody Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created. Performing all operations being allowed only in the calibration mode Maintain the roles as defined in {UIA_208} as User Groups
O.Software_Analysis	<b>FPT_PHP.3</b>	Ensures Resistance to physical attack to the TOE software in the field after the TOE activation
	<b>FPR_UNO.1</b> <b>FDP_ACC.1/FUN</b>  <b>FDP_ACC.1/SW-</b>	Ensures unobservability of secrets Defines security attributes for SFP FUNCTION according to the modes of operation Defines security attributes for SFP SW-Upgrade



Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by winfried.rogenz@continental-corporation.com	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
	Document key	Pages 85 of 106	
Villingen-Schwenningen (VIL)		Copyright (C) Continental AG 2008	

# DTCO 1381 Security Target

security objectives	Security functional requirement	
	<p><b>Upgrade</b></p> <p><b>FDP_ACF.1/FUN</b></p> <p><b>FDP_ACF.1/SW-Upgrade</b></p> <p><b>FDP_ITC.2/SW-Upgrade</b></p> <p><b>FMT_MSA.3/FUN</b></p> <p><b>FMT_MSA.3/SW-Upgrade</b></p>	<p>Defines security attributes for SFP FUNCTION according to the modes of operation</p> <p>Defines security attributes for SFP SW-Upgrade</p> <p>Provides import of user data, from outside of the TOE using the SFP SW-Upgrade. : Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected.</p> <p>Provides the SFP FUNCTION to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p>Provides the SFP SW_Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p>
	<p><b>FPT_TDC.1/SW-Upgrade</b></p>	<p>Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer</p>
<p>O.Software_Upgrade</p>	<p><b>FCS_COP.1/TDES</b></p> <p><b>FCS_COP.1/RSA</b></p> <p><b>FCS_CKM.1</b></p> <p><b>FCS_CKM.3</b></p> <p><b>FCS_CKM.4</b></p> <p><b>FDP_ITC.2/SW-Upgrade</b></p> <p><b>FDP_ACC.1/ SW-Upgrade</b></p>	<p>Provides the cryptographic operation TDES.</p> <p>Provides the cryptographic operation RSA</p> <p>Generates of session keys for the motion sensor and the tachograph cards</p> <p>Controls cryptographic key access and storage in the TOE</p> <p>Destroys cryptographic keys in the TOE</p> <p>Provides import of user data, from outside of the TOE using the SFP SW-Upgrade. : Only user data recognized as an authentic SW-Upgrade are allowed to be accepted as executable code; else they are rejected</p> <p>SFP SW-Upgrade for the upgrade of the software in the TOE</p>

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by <a href="mailto:winfried.rogenz@continental-corporation.com">winfried.rogenz@continental-corporation.com</a>	Date 2015-02-11	Department I CVAM TTS LRH	Sign
Released by <a href="mailto:winfried.rogenz@continental-corporation.com">winfried.rogenz@continental-corporation.com</a>	Date 2015-02-11	Department I CVAM TTS LRH	
	Designation DTCO 1381 Security Target		
	Document key	Pages 86 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008	

# DTCO 1381 Security Target

security objectives	Security functional requirement
	<p><b>FDP_ACF.1/SW-Upgrade</b> Defines security attributes for SFP SW-Upgrade</p> <p><b>FMT_MSA.3/SW-Upgrade</b> Provides the SFP SW_Upgrade to provide restrictive default values for security attributes that are used to enforce the SFP and allows nobody to specify alternative initial values to override the default values when an object or information is created.</p> <p><b>FPT_TDC.1/SW-Upgrade</b> Provides the capability to consistently interpret secure attributes as defined by the proprietary specification for the SW-Upgrade by the TOE developer</p>

1

## 2 9.3.2 Rationale for SFR's Dependencies

3 The dependency analysis for the security functional requirements shows that the basis for mutual  
 4 support and internal consistency between all defined functional requirements is satisfied. All  
 5 dependencies between the chosen functional components are analysed, and non-dissolved  
 6 dependencies are appropriately explained.


7 The dependency analysis has directly been made within the description of each SFR in sec.9.1 above.  
 8 All dependencies being expected by CC part 2 are either fulfilled or their non-fulfilment is justified..

## 9 9.3.3 Security Assurance Requirements Rationale

10 The current security target is claimed to be conformant with the assurance package E3hCC31\_AP (cf.  
 11 sec. 5.3 above). As already noticed there in sec. 9.2, the assurance package E3hCC31\_AP represents  
 12 the standard assurance package EAL4 augmented by the assurance components ATE\_DPT.2 and  
 13 AVA\_VAN.5.

14 The main reason for choosing made is the legislative framework [JIL], where the assurance level  
 15 required is defined in from of the assurance package E3hAP (for CCv2.1). The PP [PP] translated this  
 16 assurance package E3hAP into the assurance package E3hCC31\_AP. These packages are  
 17 commensurate with each other.

The current assurance package was chosen based on the pre-defined assurance package EAL4. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign
	Designation DTCO 1381 Security Target	Document key <span style="float: right;">Pages</span> <span style="float: right;">87 of 106</span>				
	Villingen-Schwenningen (VIL) <span style="float: right;">Copyright ( C ) Continental AG 2008</span>					

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization of the holder of the rights are prohibited. Continental AG is not liable for payment of damages. All rights reserved. Patent grant or registration of a utility model or design patent are reserved.

# DTCO 1381 Security Target

- 1 The selection of the component ATE\_DPT.2 provides a higher assurance than the pre-defined EAL4  
 2 package due to requiring the functional testing of SFR-enforcing modules.
- 3 The selection of the component AVA\_VAN.5 provides a higher assurance than the pre-defined EAL4  
 4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks  
 5 performed by an attacker possessing a high attack potential (see also Table 3: Subjects and external  
 6 entities, entry 'Attacker'). This decision represents a part of the conscious security policy for the  
 7 recording equipment required by the legislative [3821\_IB] and reflected by the current ST.
- 8 The set of *assurance* requirements being part of EAL4 fulfils all dependencies a priori.
- 9 The augmentation of EAL4 chosen comprises the following assurance components:
- 10 – ATE\_DPT.2 and  
 11 – AVA\_VAN.5.
- 12 For these additional assurance component, all dependencies are met or exceeded in the EAL4  
 13 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependency fulfilled by
<b>TOE security assurance requirements (only additional to EAL4)</b>		
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2


14 **Table 6 SAR Dependencies**

## 15 9.3.4 Security Requirements – Internal Consistency

16 The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form an internally consistent whole.

### a) SFRs

The dependency analysis in section 9.3.2 Rationale for SFR's Dependencies for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
Document key						Pages 88 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			



# DTCO 1381 Security Target

---


1 All subjects and objects addressed by more than one SFR in sec. 9.1 are also treated in a  
 2 consistent way: the SFRs impacting them do not require any contradictory property and  
 3 behaviour of these 'shared' items. The current PP accurately and completely reflects the  
 4 Generic Security Target 3821\_IB\_10]]. Since the GST 3821\_IB\_10] is part of the related  
 5 legislation, it is assumed to be internally consistent. Therefore, due to conformity between the  
 6 current ST and 3821\_IB\_10], also subjects and objects being used in the current ST are used  
 7 in a consistent way.

## 8 b) SARs

9 The assurance package EAL4 is a pre-defined set of internally consistent assurance  
 10 requirements. The dependency analysis for the sensitive assurance components in section  
 11 9.3.3 Security Assurance Requirements Rationale shows that the assurance requirements  
 12 are internally consistent, because all (additional) dependencies are satisfied and no  
 13 inconsistency appears.

14 Inconsistency between functional and assurance requirements could only arise, if there are  
 15 functional-assurance dependencies being not met – an opportunity having been shown not to  
 16 arise in sections 9.3.2 Rationale for SFR's Dependencies and 9.3.3 Security Assurance  
 17 Requirements Rationale. Furthermore, as also discussed in section 9.3.3 Security  
 18 Assurance Requirements Rationale, the chosen assurance components are adequate for  
 19 the functionality of the TOE. So, there are no inconsistencies between the goals of these two  
 20 groups of security requirements.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						89 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

## 1 10 TOE summary specification

2 The TOE provides the following security services:

**TOE\_SS.Identification\_Authentication** The TOE provides this security service of identification and authentication of the motion sensor, of users by monitoring the tachograph cards.

Detailed properties of this security service are described in Annex A (Requirements UIA\_201 to UIA\_223 as defined in 3821\_IB\_10]

### Security functional requirements concerned:

- FIA\_UID.2/MS: Identification of the motion sensor
- FIA\_UID.2/TC: Identification of the tachograph cards
- (FIA\_UAU.2//MS, FIA\_UAU.3/MS, FIA\_UAU.6/MS): Authentication of the motion sensor
- (FIA\_UAU.1/TC, FIA\_UAU.3/TC, FIA\_UAU.5//TC, FIA\_UAU.6/TC): Authentication of the tachograph cards
- FIA\_UAU.1/PIN: additional PIN authentication for the workshop card
- FIA\_AFL.1/MS: Authentication failure: motion sensor
- FIA\_AFL.1/TC: Authentication failure: tachograph cards
- (FIA\_ATD.1//TC, FMT\_SMR.1//TC): User groups to be maintained by the TOE

FMT\_MSA.3/FUN

FDP\_ACC.1/FUN functions

FIA\_UID.1/MD, FIA\_UID.2/MD, FIA\_UID.3/MD: user Identity management device


Supported by:

- FCS\_COP.1/TDES: for the motion sensor
- FCS\_COP.1/RSA: for the tachograph cards
- (FCS\_CKM.1, FCS\_CKM.2, FCS\_CKM.3, FCS\_CKM.4): cryptographic key management
- FAU\_GEN.1: Audit records: Generation
- (FMT\_MSA.1, FMT\_SMF.1)

**TOE\_SS.Access**

The TOE provides this security service of access control for access to functions and data of the TOE according to the

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						90 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

mode of operation selection rules.

Detailed properties of this security service are described in Annex A (Requirements ACC\_201 to ACC\_211 as defined in 3821\_IB\_10]

**Security functional requirements concerned:**

- (FDP\_ACC.1/FIL, FDP\_ACF.1/FIL): file structures
- (FDP\_ACC.1/FUN, FDP\_ACF.1/FUN): functions
- (FDP\_ACC.1/DAT, FDP\_ACF.1/DAT): stored data
- (FDP\_ACC.1/UDE, FDP\_ACF.1/UDE): user data export
- (FDP\_ACC.1/IS, FDP\_ACF.1/IS): input sources

Supported by:

- (FIA\_UAU.2//MS, FIA\_UAU.3//MS, FIA\_UAU.6//MS): Authentication of the motion sensor
- (FIA\_UAU.1//TC, FIA\_UAU.3//TC, FIA\_UAU.5//TC, FIA\_UAU.6//TC): Authentication of the tachograph cards
- FIA\_UAU.1//PIN: additional PIN authentication for the workshop card
- FMT\_MSA.3//FIL
- FMT\_MSA.3//FUN
- FMT\_MSA.3//DAT
- FMT\_MSA.3//UDE
- FMT\_MSA.3//IS
- (FMT\_MSA.1, FMT\_SMF.1, FMT\_SMR.1//TC)

TOE\_SS.Accountability

The TOE provides this security service of accountability for collection of accurate data in the TOE.


Detailed properties of this security service are described in Annex A (Requirement ACT\_201 to ACT\_207 as defined in 3821\_IB\_10]

**Security functional requirements concerned:**

- FAU\_GEN.1: Audit records: Generation
- FAU\_STG.1: Audit records: Protection against modification
- FAU\_STG.4: Audit records: Prevention of loss
- FDP\_ETC.2: Export of user data with security attributes

Supported by:

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						91 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

TOE\_SS.Audit

- (FDP\_ACC.1/DAT, FDP\_ACF.1/DAT): VU identification data
- (FDP\_ACC.1/UDE, FDP\_ACF.1/UDE): Data update on the TC
- FPT\_STM.1: time stamps
- FCS\_COP.1/TDES: for the motion sensor and the tachograph cards

The TOE provides this security service of audit related to attempts to undermine the security of the TOE and provides the traceability to associated users.

Detailed properties of this security service are described in Annex A (Requirements AUD\_201 to AUD\_205 as defined in 3821\_IB\_10]

**Security functional requirements concerned:**

- FAU\_GEN.1: Audit records: Generation
- FAU\_SAR.1: Audit records: Capability of reviewing
- FPT\_PHP.1//Seal Passive detection of physical attack
- Supported by:
- (FDP\_ACC.1/DAT, FDP\_ACF.1/DAT): Storing motion sensor’s audit records
- FDP\_ETC.2 Export of user data with security attributes: Related audit records to the TC.

TOE\_SS.Object\_Reuse

The TOE provides this security service of object reuse to ensure that temporarily stored sensitive objects are destroyed.

Detailed properties of this security service are described in Annex A (Requirement REU\_201 as defined in). 3821\_IB\_10]

**Security functional requirements concerned:**


- FDP\_RIP.1 Subset residual information protection
- Supported by:
- FCS\_CKM.4: Cryptographic key destruction

TOE\_SS.Reliability

The TOE provides this security service of reliability of service: self-tests, no way to analyse or debug software in the field, detection of specified hardware sabotage and deviations from the specified voltage values including cut-off of the power supply.

Detailed properties of this security service are described in Annex A (Requirements RLB\_201 to RLB\_215 as defined in). 3821\_IB\_10]

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent, grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						92 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

**Security functional requirements concerned:**

- FDP\_ITC.2//IS: no executable code from external sources
- FPR\_UNO.1: Unobservability of leaked data
- FPT\_FLS.1: Failure with preservation of secure state
- FPT\_PHP.1//Seal Passive detection of physical attack
- FPT\_PHP.2//Power\_Deviation: Notification of physical attack
- FPT\_PHP.3: Resistance to physical attack: stored data
- FPT\_TST.1: TSF testing
- FRU\_PRS.1: Availability of services
- FDP\_ACC.1/SW-Upgrade
- FDP\_ACF.1/SW-Upgrade
- FDP\_ITC.2/SW-Upgrade
- FPT\_TDC.1/SW-Upgrade
- FMT\_MSA.3SW-Upgrade
- Supported by:
  - FAU\_GEN.1: Audit records: Generation
  - (FDP\_ACC.1/IS, FDP\_ACF.1/IS): no executable code from external sources
  - (FDP\_ACC.1/FUN, FDP\_ACF.1/FUN): Tachograph Card withdrawal
  - FMT\_MOF.1: No test entry points

TOE\_SS.Accuracy


The TOE provides this security service of accuracy of stored data in the TOE.

Detailed properties of this security service are described in Annex A (Requirements ACR\_201 to ACR\_205 as defined in 3821\_IB\_10]

**Security functional requirements concerned:**

- FDP\_ITC.1: right input sources without sec. attributes (keyboard, calibration data, RTC)
- FDP\_ITC.2//IS: right input sources with sec. attributes (MS and TC)
- FPT\_TDC.1//IS: Inter-TSF basic TSF data consistency (MS and TC)

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com		2015-02-11		I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						93 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

- FDP\_SDI.2: Stored data integrity

Supported by:

- (FDP\_ACC.1/IS, FDP\_ACF.1/IS): right input sources
- (FDP\_ACC.1/FUN, FDP\_ACF.1/FUN): limited manual entry
- FAU\_GEN.1: Audit records: Generation
- FPT\_STM.1: Reliable time stamps
- (FIA\_UAU.2//MS, FIA\_UAU.3/MS, FIA\_UAU.6/MS): Authentication of the motion sensor
- (FIA\_UAU.1/TC, FIA\_UAU.3/TC, FIA\_UAU.5//TC, FIA\_UAU.6/TC): Authentication of the tachograph cards

TOE\_SS.Data\_Exchange


The TOE provides this security service of data exchange with the motion sensor and tachograph cards and connected entities for downloading.

Detailed properties of this security service are described in Annex A (Requirement DEX\_201 to DEX\_208 as defined in 3821\_IB\_10]).

**Security functional requirements concerned:**

- FCO\_NRO.1: Selective proof of origin for data to be downloaded to external media
- FDP\_ETC.2 Export of user data with security attributes: to the TC and to external media
- FDP\_ITC.2//IS Import of user data with security attributes: from the MS and the TC
- Supported by:
  - FCS\_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging)
  - FCS\_COP.1/RSA: for data downloading to external media (signing)
  - (FCS\_CKM.1, FCS\_CKM.2, FCS\_CKM.3, FCS\_CKM.4): cryptographic key management
  - (FDP\_ACC.1/UDE, FDP\_ACF.1/UDE): User data export to the TC and to external media
  - (FDP\_ACC.1/IS, FDP\_ACF.1/IS): User data import from the MS and the TC
  - FAU\_GEN.1: Audit records: Generation

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						94 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

---

TOE\_SS.Cryptographic\_support

The TOE provides this security service of cryptographic support using standard cryptographic algorithms and procedures.

Detailed properties of this security service are described in Annex A (Requirement CSP\_201 to CSP\_205 as defined in 3821\_IB\_10]).

**Security functional requirements concerned:**

- FCS\_COP.1/TDES: for the motion sensor and the tachograph cards (secure messaging)
- FCS\_COP.1/RSA: for data downloading to external media (signing)
- (FCS\_CKM.1, FCS\_CKM.2, FCS\_CKM.3, FCS\_CKM.4): cryptographic key management

1  
2  
3  
4  
5  
6  
7  
8  
9


**Application Note 26:** The following requirements of the generic security target 3821\_IB\_10] are not fulfilled by the TOE security services:

-UIA\_202: is covered by OSP.Type\_Approved\_MS

-ACR\_202. ACR\_203 are not applicable because the TOE is a single protected entity.

-RLB\_207, RLB\_208: the optional list of the hardware sabotage events in the sense of this requirement represents an empty set for the current TOE.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 95 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

## 1 11 Reference documents

- 2 [16844-3].....**ISO 16844-3**, Road vehicles, Tachograph systems, Part 3: Motion sensor inter-  
 3 face, First edition, 2004-11-01, Corrigendum 1, 2006-03-01
- 4 [2135].....**Council Regulation (EC) No. 2135/98** of 24. September 1998 amending  
 5 Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC  
 6 concerning the application of Regulations (EEC) No 3820/85 and (EEC) No 3821/85
- 7 [3821].....**Council Regulation (EEC) No. 3821/85** of the 20. December 1985 on re-  
 8 cording equipment in road transport.
- 9 [3821\_IB].....**Annex IB** of Council Regulation (EEC) No. 3821/85 amended by CR (EC) No.  
 10 1360/2002 and last amended by CR (EU) No. 1266/2009
- 11 [3821\_IB\_1].....**Appendix 1** of Annex I B of Council Regulation (EEC) No. 3821/85 -  
 12 Data Dictionary
- 13 [3821\_IB\_2].....**Appendix 2** of Annex I B of Council Regulation (EEC) No. 3821/85 -  
 14 Tachograph Cards Specification
- 15 [3821\_IB\_10].....**Appendix 10** of Annex I B of Council Regulation (EEC) No. 3821/85 -  
 16 Generic Security Targets
- 17 [3821\_IB\_11].....**Appendix 11** of Annex I B of Council Regulation (EEC) No. 3821/85 -  
 18 Common security mechanisms
- 19 [CC].....**Common Criteria** for Information Technology Security Evaluation, version 3.1,  
 20 Revision 4, September 2012, CCMB-2012-09-(01 to 03)
- 21 [CC\_1].....**Common Criteria** for Information Technology Security Evaluation, Part 1:  
 22 Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- 23 [CC\_2].....**Common Criteria** for Information Technology Security Evaluation, Part 2:  
 24 Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2009
- 25 [CC3].....**Common Criteria** for Information Technology Security Evaluation, Part3:  
 26 Security Assurance Requirements CCMB-2012-09-003, Version 3.1, Revision 4, September 2009
- 27 [CEM].....**Common Methodology** for Information Technology Security Evaluation,  
 28 Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2009
- 29 [DES] .....**Data, Encryption Standard**. National Institute of Standards and Technology  
 30 (NIST). FIPS Publication 46-3:.Draft 1999
- [JIL].....**Joint Interpretation Library**. Security Evaluation and Certification of Digital  
 Tachographs. JIL interpretation of the Security Certification according to Commission Regulation (EC)  
 1360/2002, Annex 1B, Version 1.12, June 2003
- [1360].....**Commission Regulation (EC) No 1360/2002** of 13 June 2002 adapting for the  
 seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in  
 road transport

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights reserved by Continental AG. Registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation				Pages	
		DTCO 1381 Security Target				96 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			




# DTCO 1381 Security Target

---

- 1 [ISO 7816-4].....ISO/IEC 7816-4 Information technology . Identification cards. Integrated cir-
- 2 cuit(s) cards with contacts. Part 4: Interindustry commands for interexchange. First edition: 1995 +
- 3 Amendment 1: 1997.
- 4 [ISO 7816-8].....ISO/IEC 7816-8 Information technology . Identification cards . Integrated cir-
- 5 cuit(s) cards with contacts. Part 8: Security related interindustry commands. First Edition: 1999.
- 6 [SHA-1] .....SHA-1 National Institute of Standards and Technology (NIST). FIPS Publication
- 7 180-1: Secure Hash Standard. April 1995
- 8 [PKCS1]] ..... RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. October
- 9 1998Annex A
- 10 [PP]..... Common Criteria Protection Profile, Digital Tachograph – Vehicle Unit (VU
- 11 PP),BSI-CC-PP-0057, Version 1.0, 13<sup>th</sup> July 2010, Bundesamt für Sicherheit in der
- 12 Informationstechnik,
- 13

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by <a href="mailto:winfried.rogenz@continental-corporation.com">winfried.rogenz@continental-corporation.com</a> Released by <a href="mailto:winfried.rogenz@continental-corporation.com">winfried.rogenz@continental-corporation.com</a>	Date 2015-02-11 2015-02-11	Department I CVAM TTS LRH I CVAM TTS LRH	Sign
• Designation <b>DTCO 1381 Security Target</b>			
		Document key	Pages <b>97 of 106</b>
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008	

# DTCO 1381 Security Target

## 1 12 Annex A

2 The following table demonstrates the coverage of the requirements of 3821\_IB\_10] chapter 4  
 3 by the security functional requirements from [CC], part2 specified in section 9.1.  
 4


Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	<b>TOE_SS.Identification &amp; Authentication</b>	
UIA_201	The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to.	FIA_UID.2/MS
UIA_202	The identity of the motion sensor shall consist of the sensor approval number and the sensor serial number.	OSP.Type_Approved_MS
UIA_203	The VU shall authenticate the motion sensor it is connected to: - at motion sensor connection, - at each calibration of the recording equipment, - at power supply recovery. Authentication shall be mutual and triggered by the VU.	FIA_UAU.2/MS
UIA_204	The VU shall periodically ( <i>period TBD by manufacturer: every 30 seconds, in power save mode up to 45 minutes and more frequently than once per hour</i> ) re-identify and re-authenticate the motion sensor it is connected to, and ensure that the motion sensor identified during the last calibration of the recording equipment has not been changed.	FIA_UAU.6/MS
UIA_205	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/MS
UIA_206	After ( <i>TBD by manufacturer: 2 and not more than 20</i> ) consecutive unsuccessful authentication attempts have been detected, and/or after detecting that the identity of the motion sensor has changed while not authorised (i.e. while not during a calibration of the recording equipment), the SEF shall: - generate an audit record of the event, - warn the user, - continue to accept and use non secured motion data sent by the motion sensor.	FIA_AFL.1/MS, FAU_GEN.1
UIA_207	The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.	FIA_UID.2/TC
UIA_208	The user identity shall consist of: - a user group: - DRIVER (driver card), - CONTROLLER (control card), - WORKSHOP (workshop card),	FIA_ATD.1/TC for User Identity  FMT_MSA.3/FUN for the default value UNKNOWN (no valid card)  FDP_ACC.1/FUN for functions (for UNKNOWN)

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 98 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	<ul style="list-style-type: none"> <li>- COMPANY (company card),</li> <li>- UNKNOWN (no card inserted),</li> <li>- a user ID, composed of :                             <ul style="list-style-type: none"> <li>- the card issuing Member State code and of the card number,</li> <li>- UNKNOWN if user group is UNKNOWN.</li> </ul> </li> </ul> UNKNOWN identities may be implicitly or explicitly	FMT_MSA.1 FMT_MSA.3/FUN FMT_SMF.1 FMT_SMR.1/TC for five different User Groups
UIA_209	The VU shall authenticate its users at card insertion.	FIA_UAU.1/TC
UIA_210	The VU shall re-authenticate its users: <ul style="list-style-type: none"> <li>- at power supply recovery,</li> <li>- periodically or after occurrence of specific events (<i>TBD by manufacturers: every 12 hours and more frequently than once per day</i>).</li> </ul>	FIA_UAU.6/TC
UIA_211	Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute.  Authentication shall be mutual and triggered by the VU.	FIA_UAU.5/TC
UIA_212	In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PINs shall be at least 4 characters long.  Note: In the case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer.	FIA_UAU.1/PIN
UIA_213	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/TC
UIA_214	After 5 consecutive unsuccessful authentication attempts have been detected, the SEF shall: <ul style="list-style-type: none"> <li>- generate an audit record of the event,</li> <li>- warn the user,</li> </ul> assume the user as UNKNOWN, and the card as non valid (definition z) and requirement 007).	FIA_AFL.1/TC, FAU_GEN.1
UIA_215	For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.	FIA_UID.2/TC
UIA_216	The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number.	FIA_ATD.1/TC


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation DTCO 1381 Security Target					
		Document key				Pages 99 of 106	
Villingen-Schwenningen (VIL)				Copyright ( C ) Continental AG 2008			

# DTCO 1381 Security Target

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
UIA_217	The VU shall successfully authenticate the remotely connected company before allowing any data export to it.	FIA_UAU.1/TC
UIA_218	Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute.	FIA_UAU.5/TC
UIA_219	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/TC
UIA_220	After 5 consecutive unsuccessful authentication attempts have been detected, the VU shall:  warn the remotely connected company.	FIA_AFL.1/Remote
UIA_221	For every interaction with a management device, the VU shall be able to establish the device identity.	FIA_UID.2/MD
UIA_222	Before allowing any further interaction, the VU shall successfully authenticate the management device.	FIA_UAU.1/MD
UIA_223	The VU shall detect and prevent use of authentication data that has been copied and replayed.	FIA_UAU.3/MD
	<b>TOE_SS.Access Control</b>	
ACC_201	The VU shall manage and check access control rights to functions and to data.	FDP_ACC.1/FUN for functions FMT_MSA.3/FUN FDP_ACC.1/DAT for data FMT_MSA.3/DAT
ACC_202	The VU shall enforce the mode of operation selection rules (requirements 006 to 009).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for choosing an operation mode according to REQ006 to 009.
ACC_203	The VU shall use the mode of operation to enforce the functions access control rules (requirement 010).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for accessible functions in each mode of operation (REQ010)
ACC_204	The VU shall enforce the VU identification data write access rules (requirement 076)	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ076 FMT_MSA.3/DAT
ACC_205	The VU shall enforce the paired motion sensor identification data	FDP_ACC.1/DAT


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation					
		DTCO 1381 Security Target					
		Document key				Pages	
						100 of 106	
Villingen-Schwenningen (VIL)		Copyright ( C ) Continental AG 2008					

# DTCO 1381 Security Target

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	write access rules (requirements 079 and 155)	FDP_ACF.1/DAT with a set of rules for REQ079 and 155 FMT_MSA.3/DAT
ACC_206	After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory (requirements 154 and 156).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for REQ154 and 156.
ACC_207	After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097).	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ097 FMT_MSA.3/DAT
ACC_208	After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158).	FDP_ACC.1/FUN FDP_ACF.1/FUN with a set of rules for ACC_208
ACC_209	<i>After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100).</i>	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for ACC_209 FMT_MSA.3/DAT
ACC_210	The VU shall enforce appropriate read and write access rights to security data (requirement 080).	FDP_ACC.1/DAT FDP_ACF.1/DAT with a set of rules for REQ080 FMT_MSA.3/DAT
ACC_211	Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.	FDP_ACC.1/FIL and FDP_ACF.1/FIL with only one rule as stated in ACC_211 for file structure FMT_MSA.3/FIL
	<b>TOE_SS.Accountability</b>	
ACT_201	The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087 105a, 105b 109 and 109a).	FAU_GEN.1 with an entry for REQ081, 084, 087, 105a FAU_STG.4 for REQ105b FDP_ACC.1/UDE FDP_ACF.1/UDE


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages			
Villingen-Schwenningen (VIL)				101 of 106			
				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target


Requirement Appendix 10	Requirement Description	related SFR used in the current ST
		FDP_ETC.2 FMT_MSA.3/UDE
ACT_202	The VU shall hold permanent identification data (requirement 075).	FDP_ACC.1/DAT, FDP_ACF.1/DAT FMT_MSA.3/DAT
ACT_203	The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).	FAU_GEN.1 with an entry for REQ098, 101 FDP_ACC.1/UDE FDP_ACF.1/UDE FDP_ETC.2 for REQ109 FMT_MSA.3/UDE
ACT_204	The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109).	FAU_GEN.1 with an entry for REQ102, 103 FDP_ACC.1/UDE FDP_ACF.1/UDE FDP_ETC.2 for REQ109 FMT_MSA.3/UDE
ACT_205	The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).	FAU_GEN.1 with an entry for REQ 090, 093
ACT_206	The VU shall ensure that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data.	FAU_STG.1 with <i>detection</i> for 081 to 093 and 102 to 105a FAU_STG.4 for REQ105b
ACT_207	The VU shall ensure that it does not modify data already stored in a tachograph card (requirement 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in Appendix 1 Paragraph 2.1.Note.	FDP_ETC.2 for REQ109, 109a and 110
	<b>TOE_SS.Audit</b>	
AUD_201	The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109).	FAU_GEN.1 for REQ094, 096 FDP_ETC.2
AUD_202	The events affecting the security of the VU are the following: <ul style="list-style-type: none"> <li>- Security breach attempts: <ul style="list-style-type: none"> <li>- motion sensor authentication failure,</li> <li>- tachograph card authentication failure,</li> <li>- unauthorised change of motion sensor,</li> </ul> </li> </ul>	FAU_GEN.1 for AUD_202

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages 102 of 106			
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target


Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	<ul style="list-style-type: none"> <li>- card data input integrity error,</li> <li>- stored user data integrity error,</li> <li>- internal data transfer error,</li> <li>- unauthorised case opening,</li> <li>- hardware sabotage,</li> </ul> <ul style="list-style-type: none"> <li>- Last card session not correctly closed,</li> <li>- Motion data error event,</li> <li>- Power supply interruption event,</li> <li>- VU internal fault.</li> </ul>	
AUD_203	The VU shall enforce audit records storage rules (requirement 094 and 096).	FAU_GEN.1
AUD_204	The VU shall store audit records generated by the motion sensor in its data memory.	FDP_ACC.1/DAT FDP_ACF.1/DAT FMT_MSA.3/DAT
AUD_205	It shall be possible to print, display and download audit records.	FAU_SAR.1
	F.Object Reuse	
REU_201	The VU shall ensure that temporary storage objects can be reused without this involving inadmissible information flow.	FDP_RIP.1
	<b>TOE_SS.Accuracy</b>	
ACR_201	<p>The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources:</p> <ul style="list-style-type: none"> <li>- vehicle motion data,</li> <li>- VU's real time clock,</li> <li>- recording equipment calibration parameters,</li> <li>- tachograph cards,</li> <li>- user's inputs.</li> </ul>	FDP_ACC.1/IS FDP_ACF.1/IS FPT_STM.1 for - VU's real time clock,  FDP_ITC.1 for - recording equipment calibration parameters, - user's inputs;  FDP_ITC.2/IS for - vehicle motion data; - tachograph cards.  FPT_TDC.1/IS
ACR_201a	The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal – current insertion (requirement 050a).	FDP_ACC.1/FUN FDP_ACF.1/FUN
ACR_202	If data are transferred between physically separated parts of the	<i>Since the TOE is a single protected entity, this requirement</i>

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation		DTCO 1381 Security Target			
		Document key		Pages 103 of 106			
Villingen-Schwenningen (VIL)				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	VU, the data shall be protected from modification.	<i>does not apply</i>
ACR_203	Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.	<i>Since the TOE is a single protected entity, this requirement does not apply</i>
ACR_204	The VU shall check user data stored in the data memory for integrity errors.	FDP_SDI.2
ACR_205	Upon detection of a stored user data integrity error, the SEF shall generate an audit record.	FDP_SDI.2, FAU_GEN.1
	<b>TOE_SS.Reliability</b>	
RLB_201	a) Organisational part by manufacturer  All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation.  b) VU shall care:  It shall not be possible to restore them for later use.	FMT_MOF.1 for the property b)  The property a) is formulated as OSP.Test_Points.
RLB_202	The VU shall run self tests, during initial start-up, and during normal operation to verify its correct operation. The VU self tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).	FPT_TST.1
RLB_203	Upon detection of an internal fault during self test, the SEF shall:  – generate an audit record (except in calibration mode), – preserve the stored data integrity.	FAU_GEN.1 for an audit record  FPT_FLS.1 for preserving the stored data integrity
RLB_204	There shall be no way to analyse or debug software in the field after the VU activation.	FPT_PHP.3 and ADV_ARC (self-protection for stored data)  FPR_UNO.1 (no successful analysis of leaked data)
RLB_205	Inputs from external sources shall not be accepted as executable code.	FDP_ITC.2//IS with FDP_ACC.1//IS, FDP_ACF.1//IS  FDP_ACC.1/SW-Upgrade FDP_ACF.1/SW-Upgrade FDP_ITC.2/SW-Upgrade FPT_TDC.1/SW-Upgrade FMT_MSA.3SW-Upgrade
RLB_206	If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of 6 months. In such a	FAU_GEN.1 for auditing,  FPT_PHP.1//Seal

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.


Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages			
Villingen-Schwenningen (VIL)				104 of 106			
				Copyright (C) Continental AG 2008			



# DTCO 1381 Security Target

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
	<p>case, the SEF shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection).</p> <p>If the VU is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).</p>	
RLB_207	After its activation, the VU shall detect specified ( <i>TBD by manufacturer</i> ) hardware sabotage:	The list of the specified HW sabotage is an empty set for the current TOE. Hence, no SFR is required in order to cover this item.
RLB_208	In the case described above, the SEF shall generate an audit record and the VU shall: ( <i>TBD by manufacturer</i> ).	This requirement depends on RLB_207: If the latter is not implemented, the current requirement cannot be implemented.
RLB_209	The VU shall detect deviations from the specified values of the power supply, including cut-off.	FPT_PHP.2/Power_Deviation for detection
RLB_210	In the case described above, the SEF shall: <ul style="list-style-type: none"> <li>• generate an audit record (except in calibration mode),</li> <li>• preserve the secure state of the VU,</li> <li>• maintain the security functions, related to components or processes still operational,</li> <li>• preserve the stored data integrity.</li> </ul>	FAU_GEN.1 for auditing  FPT_FLS.1 for preserving a secure state incl. the stored data integrity and/or a clean reset (cf. also RLB_203 and RLB_211)
RLB_211	In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the VU shall be reset cleanly.	FPT_FLS.1 for preserving a secure state incl. the stored data integrity and/or a clean reset
RLB_212	The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.	FRU_PRS.1
RLB_213	The VU must ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016).	FDP_ACC.1/FUN  FDP_ACF.1/FUN with a rule for REQ015 and 016
RLB_214	In the case described above, the SEF shall generate an audit record of the event.	FAU_GEN.1 (Last card session not correctly closed)
RLB_215	If the VU provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall not share security data. Only one task shall be active at a time.	ADV_ARC (domain separation)
	<b>TOE_SS.Data Exchange</b>	


Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		• Designation		DTCO 1381 Security Target			
		Document key		Pages			
Villingen-Schwenningen (VIL)				105 of 106			
				Copyright (C) Continental AG 2008			

# DTCO 1381 Security Target

Requirement Appendix 10	Requirement Description	related SFR used in the current ST
DEX_201	The VU shall verify the integrity and authenticity of motion data imported from the motion sensor.	FDP_ITC.2/IS for – vehicle motion data;
DEX_202	Upon detection of a motion data integrity or authenticity error, the SEF shall: <ul style="list-style-type: none"> <li>• generate an audit record,</li> <li>• continue to use imported data.</li> </ul>	FAU_GEN.1. FDP_ITC.2/IS for – vehicle motion data;
DEX_203	The VU shall verify the integrity and authenticity of data imported from tachograph cards.	FDP_ITC.2/IS for – tachograph cards.
DEX_204	Upon detection of a card data integrity or authenticity error, the SEF shall: <ul style="list-style-type: none"> <li>• generate an audit record,</li> <li>• not use the data.</li> </ul>	FAU_GEN.1 FDP_ITC.2/IS for – tachograph cards.
DEX_205	The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.	FDP_ETC.2
DEX_206	The VU shall generate an evidence of origin for data downloaded to external media.	FCO_NRO.1
DEX_207	The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient.	FCO_NRO.1
DEX_208	The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.	FDP_ETC.2
	<b>TOE_SS.Cryptographic support</b>	
CSP_201	Any cryptographic operation performed by the VU shall be in accordance with a specified algorithm and a specified key size.	FCS_COP.1/TDES FCS_COP.1/RSA
CSP_202	If the VU generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes	FCS_CKM.1
CSP_203	If the VU distributes cryptographic keys, it shall be in accordance with specified key distribution methods.	FCS_CKM.2
CSP_204	If the VU accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.	FCS_CKM.3
CSP_205	If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.	FCS_CKM.4

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Designed by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH	Sign	
Released by	winfried.rogenz@continental-corporation.com	Date	2015-02-11	Department	I CVAM TTS LRH		
		Designation		DTCO 1381 Security Target			
		Document key		Pages			
Villingen-Schwenningen (VIL)				106 of 106			
				Copyright (C) Continental AG 2008			