

# DIN CEN/TR 16968:2018-12 (E)

## Electronic Fee Collection - Assessment of security measures for applications using Dedicated Short-Range Communication; English version CEN/TR 16968:2016

---

<b>Contents</b>	<b>Page</b>
European foreword.....	4
Introduction .....	5
1 Scope.....	6
2 Terms and definitions .....	6
3 Abbreviations .....	9
4 Method .....	10
5 Security Objectives and Functional Requirements.....	13
5.1 Target of evaluation .....	13
5.2 Security objectives.....	14
5.2.1 Introduction .....	14
5.2.2 Confidentiality.....	14
5.2.3 Availability .....	14
5.2.4 Accountability .....	14
5.2.5 Data integrity.....	14
5.3 Functional security requirements .....	15
5.3.1 Introduction .....	15
5.3.2 Confidentiality.....	15
5.3.3 Availability .....	17
5.3.4 Accountability .....	18
5.3.5 Data integrity.....	20
5.4 Inventory of assets.....	21
5.4.1 Functional Assets .....	21
5.4.2 Data Assets.....	22
6 Threat analysis.....	22
7 Qualitative risk analysis .....	24
7.1 Introduction .....	24
7.1.1 General.....	24
7.1.2 Likelihood of a threat .....	24
7.1.3 Impact of a threat.....	25
7.1.4 Classification of Risk.....	26
7.2 Risk determination.....	26
7.2.1 Definition of high and low risk context.....	26
7.2.2 Threat T1: Access Credentials keys can be obtained .....	27
7.2.3 Threat T2: Authentication keys can be obtained .....	27
7.2.4 Threat T3: OBU can be cloned .....	28
7.2.5 Threat T4: OBU can be faked.....	28
7.2.6 Threat T5: Authentication of OBU data can be repudiated.....	29
7.2.7 Threat T6: Application data can be modified after the transaction .....	29
7.2.8 Threat T7: Data in the VST is not secure.....	30
7.2.9 Threat T8: DSRC Communication can be eavesdropped.....	30
7.2.10 Threat T9: Correctness of application data are repudiated .....	31
7.2.11 Threat T10: Master keys may be obtained from RSE.....	31
7.3 Summary .....	31

<b>8</b>	<b>Proposals for new security measures .....</b>	<b>32</b>
<b>8.1</b>	<b>Introduction.....</b>	<b>32</b>
<b>8.2</b>	<b>Security measures to counter risks related to key recovery .....</b>	<b>32</b>
<b>8.3</b>	<b>Recommended countermeasures.....</b>	<b>34</b>
<b>8.4</b>	<b>Qualitative cost benefit analysis .....</b>	<b>35</b>
<b>9</b>	<b>Impact of proposed countermeasures.....</b>	<b>35</b>
<b>9.1</b>	<b>Current situation and level of fraud in existing EFC systems using CEN DSRC link.....</b>	<b>35</b>
<b>9.2</b>	<b>EETS legislation .....</b>	<b>36</b>
<b>9.3</b>	<b>Analysis of effects on existing EFC systems.....</b>	<b>36</b>
<b>9.3.1</b>	<b>Affected roles .....</b>	<b>36</b>
<b>9.3.2</b>	<b>The CEN DSRC equipment Manufacturers .....</b>	<b>36</b>
<b>9.3.3</b>	<b>The Toll Service Providers .....</b>	<b>37</b>
<b>9.3.4</b>	<b>The Toll Chargers .....</b>	<b>37</b>
<b>10</b>	<b>Recommendations.....</b>	<b>38</b>
<b>10.1</b>	<b>Add security levels and procedures to EN ISO 14906.....</b>	<b>38</b>
<b>10.2</b>	<b>Recommendation for other EFC standards .....</b>	<b>39</b>
<b>10.3</b>	<b>New standards .....</b>	<b>39</b>
<b>Annex A (informative)</b>	<b>Current status of the DEA cryptographic algorithm .....</b>	<b>40</b>
<b>A.1</b>	<b>Overview .....</b>	<b>40</b>
<b>A.2</b>	<b>ISO/IEC 9797-1 (MAC Algorithm 1).....</b>	<b>40</b>
<b>A.3</b>	<b>FIPS 46 (DEA Specification – DES) .....</b>	<b>40</b>
<b>A.4</b>	<b>ENISA recommendations .....</b>	<b>41</b>
<b>Annex B (informative)</b>	<b>Security considerations regarding DSRC in EFC Standards .....</b>	<b>42</b>
<b>B.1</b>	<b>Security vulnerabilities in EN 15509 and EN ISO 14906 .....</b>	<b>42</b>
<b>B.2</b>	<b>Security vulnerabilities in EN ISO 12813 (CCC) .....</b>	<b>42</b>
<b>B.3</b>	<b>Security vulnerabilities in EN ISO 13141 (LAC).....</b>	<b>43</b>
<b>B.4</b>	<b>Security vulnerabilities in CEN/TS 16702-1 (SM-CC).....</b>	<b>43</b>
	<b>Bibliography .....</b>	<b>44</b>