

# Geschäftseinheit I-ZB

## Systemführerschaft ETCS / KMC-CH

### **KMC-CH Security Policy**

### Version V1.1

Vom: 24.01.2008

	Erstellt	QS-geprüft	Freigegeben
Datum Visum	<i>Mei</i> 24.01.08	24.01.08 <i>H/H</i>	24.01.08 <i>N. Cedraschi</i>
Name	Matthias Meier	Horst Hesse	Nicolas Cedraschi
Stelle / Funktion	System Engineer	Q-Leiter	PL CKM

## Dokumenten-Kontrollblatt

Inhalt	KMC-CH Security Policy
Ersteller	M. Meier
Wordprozessor	Microsoft Word 2002
Filename	KMC_CH_Sec_Pol_V1_1.doc
Status des Dokuments	In Bearbeitung / in Review / <b><u>Freigegeben</u></b>
Verteiler	Dokument wird ad hoc durch das CKM-Team ausgeteilt

## Änderungsnachweise

Version	Datum	Ersteller	Änderungshinweise
X1.0	22.11.07	M. Meier	Erstellung des offiziellen Dokuments; Übernahme des Inhalts aus inoffizieller Version des CKM-Teams (Powerpoint-Folien); Streichung des 3. Satzes nach Rücksprache mit R. Allemann.
X1.1	10.01.08	M. Meier	Einarbeitung der Reviewkommentare von N. Cedraschi, R. Allemann und B. Wilhelm
V1.1	24.01.08	M. Meier	Freigabe

## Inhaltsverzeichnis

<b>1</b>	<b>Sicherheitsrichtlinien (deutsche Version)</b>	<b>5</b>
<b>2</b>	<b>Security Policy (english version)</b>	<b>5</b>
<b>3</b>	<b>Definitionen</b>	<b>5</b>
3.1	Deutsch	5
3.2	English	5

## Abkürzungen

KMC	Key Management Center
KMC-CH	Key Management Center Schweiz (Swiss Key Management Center)
KMAC	Schlüssel, der beim Kommunikationsaufbau zwischen 2 Endgeräten zur gegenseitigen Berechtigung als Kommunikationsinstanzen benötigt wird (Authentication Key)
KTRANS	Schlüssel, der zum Schutz des Schlüsselmaterials vor Kompromittierung beim Schlüsseltransport innerhalb des Verantwortungsbereichs eines KMC benötigt wird (Transport Key)
K-KMC	Schlüssel, der zum Schutz des Schlüsselmaterials vor Kompromittierung beim Schlüsseltransport zwischen 2 KMC benötigt wird (inter KMC transport key)

## Referenzen

- [1] UNISIG, Subset-038, Off-line Key Management FIS, V2.1.9.

# 1 Sicherheitsrichtlinien (deutsche Version)

- 1.1.1.1 Schlüssel (KMAC [1], KTRANS [1] und K-KMC [1]) dürfen nur nach Absprache mit dem Home-KMC [1] (Schlüsseleigentümer) in Klartextform oder in trivial verschlüsselter Form gespeichert oder transportiert werden.
- 1.1.1.2 Schlüssel in Klartextform oder in trivial verschlüsselter Form müssen vor unbefugtem Zugriff geschützt werden.
- 1.1.1.3 Schlüssel mit Schlüsseleigentümer KMC-CH unterliegen während ihrer gesamten Lebensdauer diesen Sicherheitsrichtlinien.

# 2 Security Policy (english version)

- 2.1.1.1 Keys (KMAC [1], KTRANS [1] and K-KMC [1]) must not be saved or transported in plaintext form or in trivially encrypted form except after authorization by the home-KMC [1] (key owner).
- 2.1.1.2 Keys in plaintext form or in trivially encrypted form must be protected against unauthorized access.
- 2.1.1.3 Keys owned by the KMC-CH are covered by the above mentioned policy over their entire lifetime.

# 3 Definitionen

## 3.1 Deutsch

- 3.1.1.1 Schlüsseleigentümer: dasjenige KMC, welches den Schlüssel erstellt hat.
- 3.1.1.2 Lebensdauer eines Crypto Keys: Zeitintervall mit Beginn „Zeitpunkt der Schlüsselgenerierung“ und Ende „Zeitpunkt der Schlüssellöschung“.

## 3.2 English

- 3.2.1.1 Key owner: the KMC that generated the key.
- 3.2.1.2 Lifetime of a crypto key: time slice beginning at the “moment of key generation” and ending at the “moment of key deletion”.