

Anleitung zum Nachladen des zentralen PV-Schlüssels für das Deutschland-Ticket



Das Nachladen der Schlüssel besteht aus den folgenden Schritten

- Schritt 0: [Vorbereitung \(S. 5\)](#)
- Schritt 1: [Erstellen einer SAM-Gruppe \(S. 6\)](#)
- Schritt 2: [Erstellen des Kryptogrammauftrages \(S. 11\)](#)
- Schritt 3: [Herunterladen der Kryptogramme \(S. 13\)](#)
- Schritt 4: [Aufspielen der Kryptogramme \(S. 16\)](#)
- Schritt 5: [Bestätigen der Kryptogramme \(S. 17\)](#)

Symmetrische Schlüssel aufs SAM nachladen

Um **symmetrische Schlüssel** über einen gesicherten Prozess auf SAMs nachzuladen, werden Kryptogramme verwendet. Diese können [im ASM-Tool](#) beauftragt werden.

Voraussetzung für die Beauftragung von Kryptogrammen:
der beauftragende Benutzer besitzt die Rolle eines Admin ASPs.

Pro Kryptogrammauftrag wird ein **Kryptogramm pro Schlüssel** und **pro SAM** erzeugt und bereitgestellt.



Für den Anschluss an das ZPV-S und das korrekte Senden der Ausgabe- und Kontrolltransaktionen wird der neue PV-Schlüssel (KID 40) der OrgID 3000 (Level 3) verwendet.

Der neue nationale PV-Schlüssel und der dazugehörige Testschlüssel (KID 40) der OrgID 35768 (Level 2) sind [im ASM-Tool](#) verfügbar.

Der nationale PV-Schlüssel muss auf die KVP-SAMs zur Ausgabe aufgebracht werden. Bitte beachten Sie ggf. auch Ihre KVP-SAMs, die bei Chipkartenherstellern und Massenpersonalisierern im Einsatz sind.

Sollten die Dienstleister-Terminals (DLT) Aktionslisten verarbeiten können, also das Aktionsmanagement implementiert sein, muss der nationale PV-Schlüssel auch auf die DL-SAMs.



Beispiel: Wird per Kryptogrammauftrag das Hinzufügen der PV-Schlüssel (KID 40) der OrgID 3000 in der Version 1 und Version 129 (also 2 Schlüssel) für 5 SAMs beauftragt, werden insgesamt 10 Kryptogramme erzeugt (2 Schlüssel x 5 SAMs = 10 Kryptogramme).

Die Entscheidung, ob Schlüssel nachgeladen oder stattdessen neue SAMs bestellt werden, ist eine wirtschaftliche und liegt bei den Verkehrsunternehmen.

Kosten lt. Preisliste (gültig ab 01.01.2022):

- pro Kryptogrammauftrag: 151,04 €
- pro SAM Level 2: 35,76 €
- pro SAM Level 3: 22,93 €
- ggf. plus Kosten für den Aufspielprozess (mit Dienstleister oder Hersteller abklären)

Schritt 0: Vorbereitung

Wenn in der Vergangenheit für die SAMs Ihres Unternehmens keine Kryptogramme beauftragt worden sind, können Sie direkt mit Schritt 1 „SAM-Gruppe erstellen“ beginnen.

Falls jedoch in der Vergangenheit Kryptogramme beauftragt worden sind, ist zunächst zu prüfen, ob es „alte“ Kryptogramme gibt, die noch nicht bestätigt worden sind.

Hintergrund: Das Nachladen der Schlüssel per Kryptogrammauftrag ist ein abgeschlossener Prozess. Erst nachdem die Schlüssel mit Kryptogrammen auf den SAMs nachgeladen und im Anschluss die Kryptogramme bestätigt worden sind, wird der Vorgang als abgeschlossen markiert.

1. Öffnen Sie das [DTS KM-Webportal](https://vdv-km-web.telesec.de/index1.html); <https://vdv-km-web.telesec.de/index1.html>
2. Anmeldung mit Anmeldedaten (OTP-Token wird hier benötigt)
3. Menüblock Kryptogramme -> Menüpunkt Bestätigen
4. Gültiges One-Time-Password (OTP) und entsprechende persönliche ServerPIN (4-stellige PIN) eingeben
5. Klicken auf Schaltfläche „Alle Bestätigen“



Abbildung 1: Bestätigen von Kryptogrammen (beispielhaft)






Weiterführende Dokumentation:
siehe [Bedienungsanleitung KM-Web-Service](#) ab S.20 ff

Schritt 1: Erstellen einer SAM-Gruppe

Da Kryptogramme für einzelne SAMs oder eine SAM-Gruppe erstellt werden können, sollte, wenn ein Schlüssel auf mehrere SAMs nachgeladen werden muss, zunächst eine SAM-Gruppe erstellt werden.

1. Anmeldung im ASM-Tool mit Benutzernamen und Benutzerkennwort
2. Klicken Sie im Menüblock auf „KM-PKI-SAM“ und wählen Sie unter „SAM-Verwaltung“ den Punkt „SAM-Gruppen“ aus
3. Wählen Sie unter „SAM-Gruppe-Typ“ einen der folgenden drei Typen aus:
 - a. SAM-Art
 - b. SAM-Bereich
 - c. SAM-Liste
4. Auswahl Schaltfläche -> SAM-Gruppe anlegen
5. Gültiges One Time Password (OTP) und entsprechende persönliche ServerPIN (4-stellige PIN) eingeben.

Neue SAM-Gruppe anlegen

SAM-Gruppe-Daten	
Org-ID*	5000 - VDV eTicket Service GmbH & Co. ▾
SAM-Gruppe-ID	wird automatisch gebildet
SAM-Gruppenname*	abc 
SAM-Gruppe-Typ*	SAM-Art ▾
SAM-Typ*	Verkauf ▾
Gültig von*	14.11.2021 
Gültig bis*	01.03.2027 
<input type="button" value="SAM-Gruppe anlegen"/> <input type="button" value="Abbrechen"/>	

*Notwendige Angaben

Abbildung 2: Anlegen einer SAM-Gruppe, Typ „SAM-Art“

zu a) „SAM-Art“: fasst SAMs entsprechend dem Typ „Verkauf“ und „Kontrolle/Erfassung“ zusammen. Bitte den gesamten Gültigkeitsbereich angeben (Gültigkeitsbeginn ist ein Tag vor dem Gültigkeitsbeginn des ersten SAMs und das Gültigkeitsende ist ein Tag nach dem Gültigkeitsende letzten SAMs zu wählen).

➡ Auf den folgenden Seiten finden Sie die [Dos and Dont's](#) zur SAM-Gruppe vom Typ SAM-Art.

zu b) „SAM-Bereich“: fasst SAMs entsprechend einem Nummernbereich zusammen. Die Nummern können dezimal bzw. hexadezimal eingegeben werden. Die bei DTS für den Kunden hinterlegten SAM Nummern werden automatisch mittels Textvervollständigung nachgeladen und lassen sich so schnell auswählen.

zu c) „SAM-Liste“: hier kann eine vorgegebene Liste von SAM-Nummern hochgeladen werden. Um eine Liste mit SAM-Nummern hochzuladen, muss diese die Struktur der SAM-Produktionsliste besitzen und als XML vorliegen. Eine SAM-Liste darf maximal 1000 SAM-Nummern beinhalten. Vor dem Hochladen der SAM-Liste werden die SAM-Nummern anhand der SAM Betreiber OrgID validiert.

Eine SAM-Liste darf keine doppelten und keine abgelaufenen SAMs beinhalten!

Der Name der XML-Datei mit der SAM-Liste darf keine Leerzeichen enthalten.



Weiterführende Dokumentation: siehe [Benutzerhandbuch ASM-Tool](#) ab S.92 ff sowie [Supportcard 30 SAM Gruppe](#) anlegen

Dos and Don'ts bei SAM-Gruppen vom Typ SAM-Art



Positiv-Beispiel: Es sollen 15 SAMs vom Typ Verkauf in einer SAM-Gruppe nach SAM-Art „Verkauf“ zusammengefasst werden (die 15 SAMs stammen aus zwei separaten SAM-Bestellungen vom 14.11.2021 und 05.01.2022)

Die SAMs aus der ersten Bestellung haben eine Gültigkeit vom 15.11.2021 bis 30.11.26 und die SAMs aus der zweiten Bestellung eine Gültigkeit vom 15.02.22 bis 31.02.27.

Durch die Eingabe der Werte 14.11.2021 und 01.03.2027 beim Anlegen der SAM-Gruppe werden alle SAMs vom Typ Verkauf, deren Gültigkeit zwischen dem 14.11.2021 und dem 01.03.2027 in dieser Gruppe zusammengefasst.

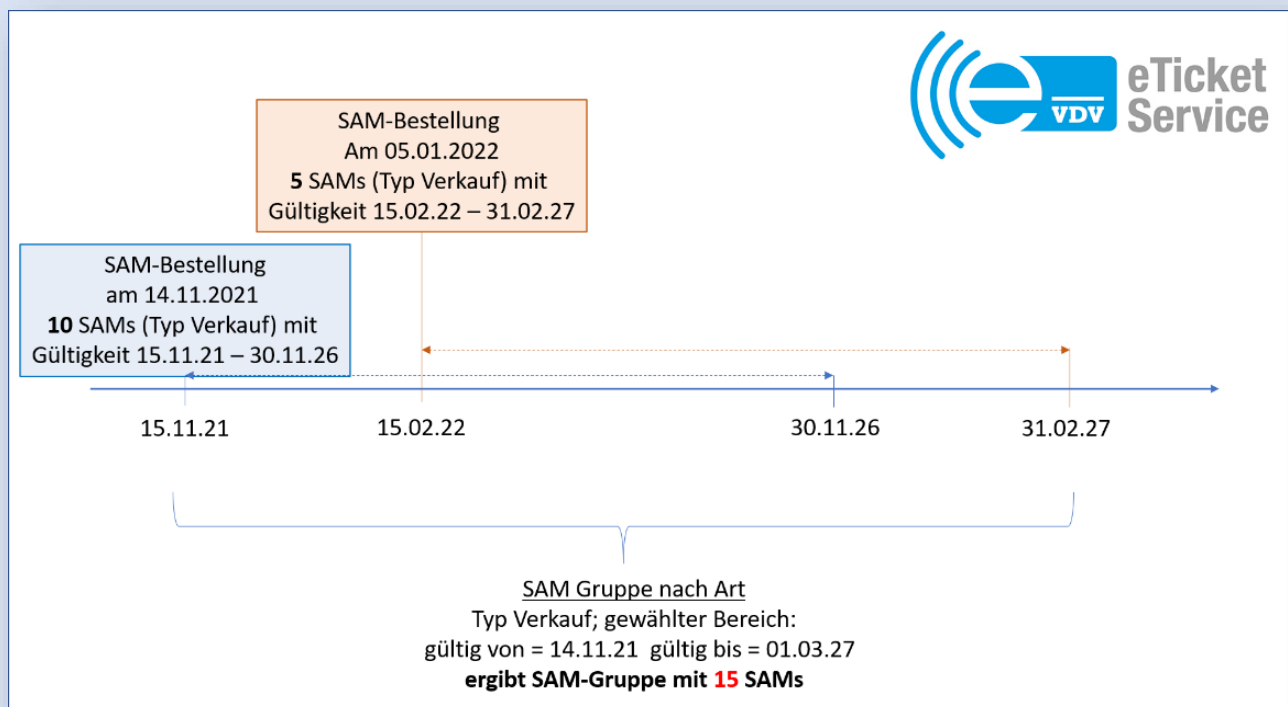


Abbildung 3: Anlegen einer SAM-Gruppe, Typ „SAM-Art“ – Gültigkeitsbereich I



Negativ-Beispiel |: Wird als Gültigkeitsbeginn der 14.11.2021 eingetragen und als Gültigkeitsende der 01.12.2026, so werden in der SAM-Gruppe nur 10 SAMs hinzugefügt, da die SAMs aus der Bestellung vom 05.02.2022 eine Gültigkeit bis zum 31.02.2027 haben und deshalb nicht in diesen Bereich fallen:

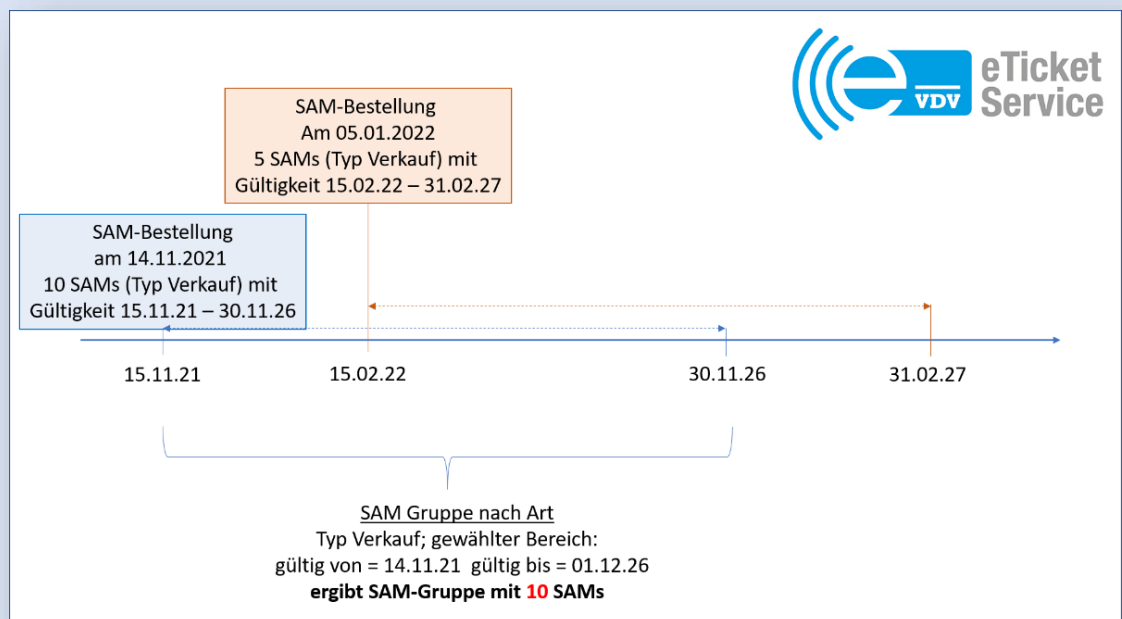


Abbildung 4: Anlegen einer SAM-Gruppe, Typ „SAM-Art“ – Gültigkeitsbereich II



Negativ-Beispiel ||: Wird als Gültigkeitsbeginn der 01.12.2021 eingetragen und als Gültigkeitsende der 01.02.2027, so werden keine SAMs in der SAM-Gruppe hinzugefügt, da die SAMs aus beiden Bestellungen nicht in diesen Gültigkeitsbereich fallen.

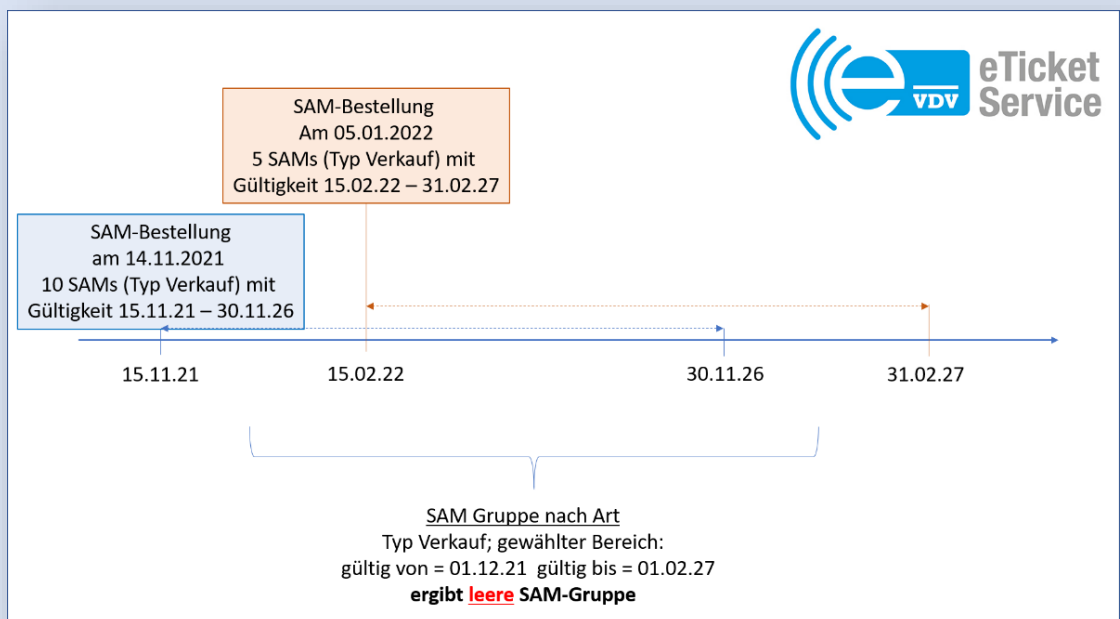


Abbildung 5 Anlegen einer SAM-Gruppe, Typ „SAM-Art“ – Gültigkeitsbereich III

Schritt 2: Erstellung des Kryptogrammauftrags

1. Anmeldung im ASM-Tool mit Benutzernamen und Benutzerkennwort
2. Klicken Sie im Menüblock auf „KM-PKI-SAM“ und wählen Sie unter „SAM-Verwaltung“ den Punkt „SAM-Kryptogrammaufträge“ aus
3. Klicken Sie auf den Button „neuen SAM-Kryptogrammauftrag erstellen“
4. Füllen Sie die Eingabemaske aus (Abbildung 6 Kryptogrammauftrag, Schlüssel auswählen und hinzufügen)
5. Geben Sie die OrgID des SAM-Eigentümers ein (d.h. Ihre eigene L2- oder L3-OrgID)
6. Wählen Sie aus, ob es sich um einen Kryptogrammauftrag für ein einzelnes SAM oder eine SAM-Gruppe handelt
7. Geben Sie den Namen der SAM-Gruppe ein
8. Im nächsten Schritt ist als Auftragstyp „Schlüssel hinzufügen“ auszuwählen
9. Bei Schlüssel-Inhaber geben Sie bitte in Abhängigkeit der gewählten eigenen OrgID für Level 3 die OrgID 3000 und für Level 2 die OrgID 35768 ein und klicken Sie auf den Button „Freigegebene Schlüssel suchen“
10. Die freigegebenen Schlüssel werden im Panel „Auswahl eines Schlüssels nach Schlüssel-Inhaber“ angezeigt.

Neuen SAM-Kryptogrammauftrag erstellen

SAM

Org-ID des SAM-Eigentümers*

E-Mail

Kryptogramm für*

SAM-Gruppe*

Auftragstyp*

Auswahl eines Schlüssels nach Schlüssel-Inhaber

Schlüssel-Inhaber* Freigegebene Schlüssel suchen

Org-ID	Kundenbezeichnung	KeyType	KeyVersion	Nutzungslimit	Aktionen
3000	VDV eTicket Service GmbH & Co. KG	PV-Schlüssel (40)	1	unbegrenzt	
3000	VDV eTicket Service GmbH & Co. KG	PV-Schlüssel (40)	129	unbegrenzt	

Ausgewählte Schlüssel

Es wurde noch kein Schlüssel ausgewählt

Abbildung 6: Kryptogrammauftrag, Schlüssel auswählen und hinzufügen

- Über das „+“ Symbol muss der Schlüssel der Version 1 (Regulärversion) und der Schlüssel der Version 129 (Notfallversion) einzeln dem Auftrag hinzugefügt werden.

Neuen SAM-Kryptogrammauftrag erstellen

SAM

Org-ID des SAM-Eigentümers*


E-Mail

Kryptogramm für*

SAM-Gruppe*

Auftragstyp*

Auswahl eines Schlüssels nach Schlüssel-Inhaber

Schlüssel-Inhaber* 

Org-ID	Kundenbezeichnung	KeyType	KeyVersion	Nutzungslimit	Aktionen
3000	VDV eTicket Service GmbH & Co. KG	PV-Schlüssel (40)	1	unbegrenzt	
3000	VDV eTicket Service GmbH & Co. KG	PV-Schlüssel (40)	129	unbegrenzt	

Ausgewählte Schlüssel


Org-ID	Kundenbezeichnung	KeyType	KeyVersion	Nutzungslimit	Aktionen
3000	VDV eTicket Service GmbH & Co. KG	PV-Schlüssel (40)	1	<input checked="" type="checkbox"/> unbegrenzt	
3000	VDV eTicket Service GmbH & Co. KG	PV-Schlüssel (40)	129	<input checked="" type="checkbox"/> unbegrenzt	

Abbildung 7: Kryptogramm-auftrag, Schlüssel auswählen und hinzufügen

- ACHTUNG: Das Nutzungslimit sollte unbegrenzt sein und nicht verändert werden.
- Klicken Sie nun auf den Button „Kryptogrammauftrag an Schlüsselinhaber senden“

Sobald die Kryptogramme erstellt sind und zum Download bereitstehen, erhalten Sie eine entsprechende Benachrichtigung per Mail.



Weiterführende Dokumentation: siehe [Benutzerhandbuch ASM-Tool](#) ab S.106 ff allgemein sowie [Supportcard 17 Kryptogrammauftrag erstellen](#).

Schritt 3: Herunterladen der Kryptogramme

1. Öffnen Sie das DTS KM-Webportal: <https://vdv-km-web.telesec.de/index1.html>
2. Anmeldung mit Anmeldedaten (OTP-Token wird hier benötigt)
3. Menüblock Kryptogramme → Menüpunkt Download
Hinweis: Sie können (**Option a**) alle Kryptogramme auf einmal herunterladen oder (**Option b**) diese einzeln nach SAMs geordnet herunterladen.



Abbildung 8: alle Kryptogramme als Paket heruntergeladen (Option a)

4. Nachdem Sie alle Kryptogramme ausgewählt haben die Sie herunterladen möchten, können Sie dies über die Schaltfläche „Herunterladen“ ausführen. Dabei werden die Dateien innerhalb einer ZIP-Datei heruntergeladen.
5. Danach werden Sie gefragt, ob die Datei direkt geöffnet oder zur Speicherung auf einem Datenträger (z.B. der Festplatte, USB-Stick, etc.) abgelegt werden soll. Wählen Sie „Öffnen“, so werden die Dateien nur in einem temporären Verzeichnis zwischengespeichert.

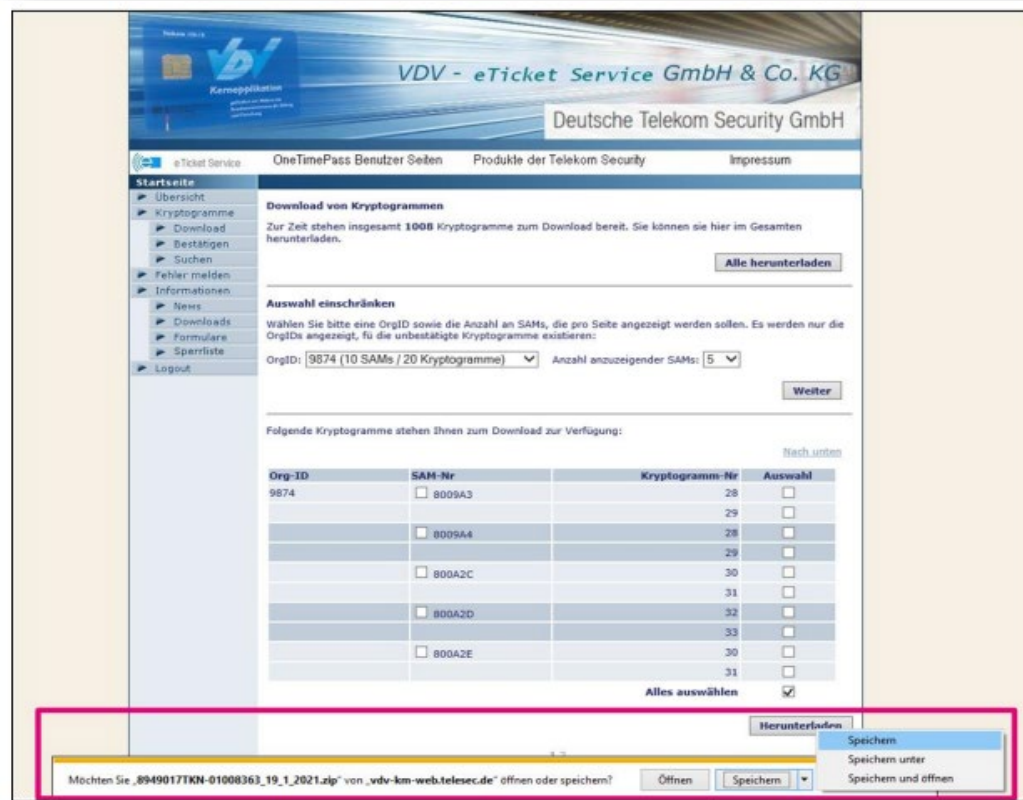


Abbildung 9: Speichern der Kryptogramme

- Im Folgenden gehen wir davon aus, dass Sie die Option „Speichern unter“ ausgewählt haben und die Datei in einem Ordner Ihrer Wahl abgelegt haben.

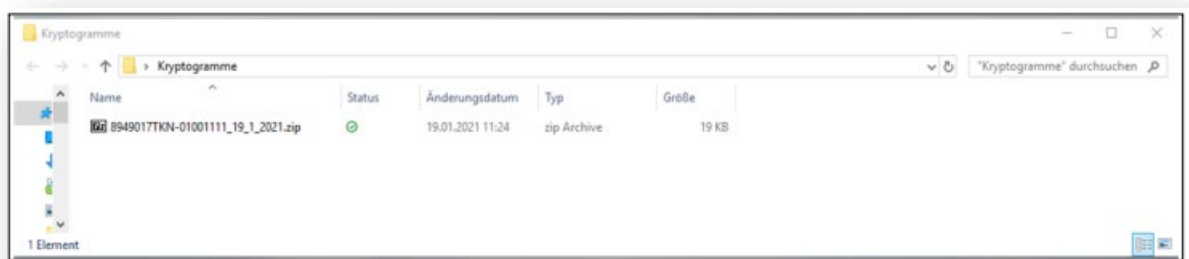


Abbildung 10: Gespeicherte Kryptogramme als ZIP-Datei

- Im oben dargestellten Beispiel wurde als Speicherort, der Ordner Kryptogramme ausgewählt. Dies ist natürlich anwenderbezogen und kann daher individuell gewählt werden. Der Dateiname wird automatisch durch die Anwendung vorgegeben, kann aber von Ihnen selbstverständlich geändert werden. Wie Sie in dem dargestellten Dateinamen (8949017TKN-01001111_19_1_2021) erkennen können, wird das Datum (..._19_1_2021) sowie die TKN-Nummer, mit welcher Sie eingeloggt sind, mitgespeichert. Auf diese Weise können Sie, falls Sie mehrere Kryptogramm-Dateien in einem Ordner haben, die einzelnen Dateien leicht identifizieren oder ordnen.

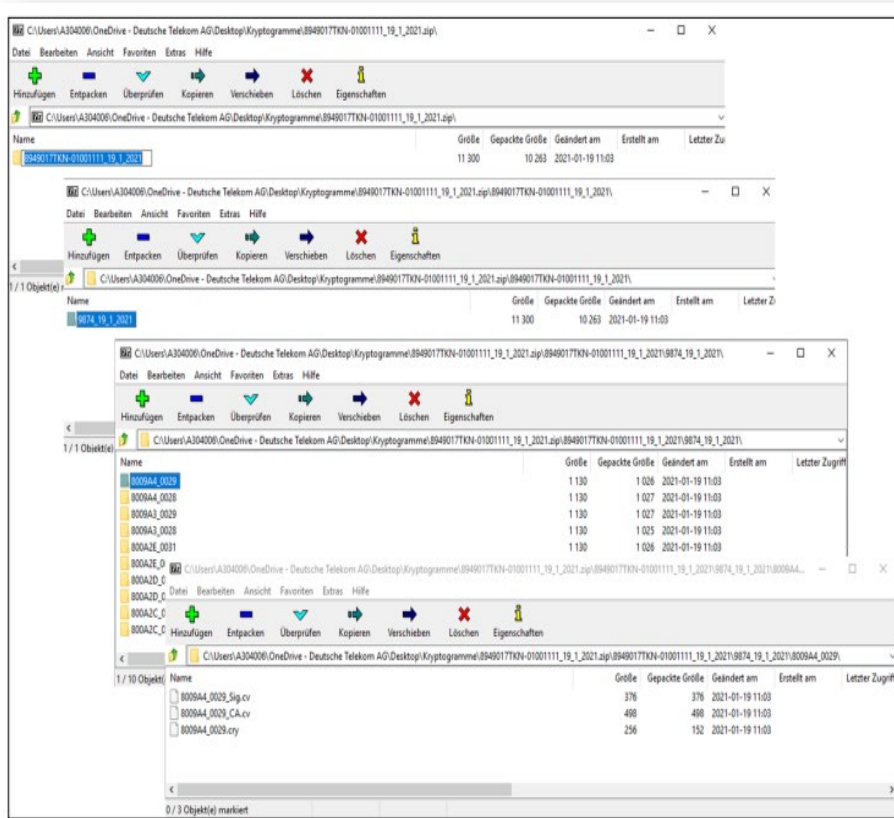


Abbildung 11: Inhalt der Downloaddateien

8. Die heruntergeladene ZIP-Datei können Sie dann in den einzelnen Ebenen öffnen. In der untersten Struktur befinden sich drei Dateien, da zu jedem Kryptogramm auch die notwendigen Dateien zur Prüfung der Signatur (Zertifikat des Signaturschlüssels und der ausstellenden CA, die für die Erstellung des Kryptogramms genutzt wurde) mitgeliefert werden.

Das dargestellte Beispiel-Kryptogramm besteht somit aus 3 Dateien:

- 1) 8009A4_0029_Sig.cv: [Signaturzertifikat des Kryptogramms](#)
- 2) 8009A4_00029_CA.cv: [CA-Zertifikat zur Prüfung des Sig.cv](#)
- 3) 8009A4_0029.cry: [eigentliches Kryptogramm](#)



Weiterführende Dokumentation: siehe [Bedienungsanleitung KM-Web-Service](#) ab S.13 ff sowie Supportcard [18 Kryptogramme herunterladen und bestätigen](#)

Schritt 4: Aufspielen der Kryptogramme

Die Kryptogramme sollten in erster Linie über die entsprechende Funktionalität der KVP- und DL-Systeme, die in der KA spezifiziert ist, eingespielt werden.

Ist dies nicht möglich, können die Kryptogramme auch mittels dem kostenfrei seitens VDV-ETS bereitgestellten LoadKey-Tool eingespielt werden. Dies erfordert aber den Aus- und Einbau der SAMs.



Download [eTT-Testtool](https://www.eticket-deutschland.de/loadkey-tool/) und [Loadkey-Tool](https://www.eticket-deutschland.de/loadkey-tool/) via Website: <https://www.eticket-deutschland.de/loadkey-tool/> oder über das [Service-Portal](https://eticket-deutschland.atlassian.net/wiki/spaces/KS/pages/46170124/eTT+Testtool) unter <https://eticket-deutschland.atlassian.net/wiki/spaces/KS/pages/46170124/eTT+Testtool>).

Beim Download des Loadkey-Tools ist auch das Handbuch enthalten.

Schritt 5: Bestätigen der Kryptogramme

1. Öffnen Sie das DTS KM-Webportal: <https://vdv-km-web.telesec.de/index1.html>
2. Anmeldung mit Anmeldedaten (OTP-Token wird hier benötigt)
3. Menüblock Kryptogramme -> Menüpunkt Bestätigen
Hinweis: Erst dann wird der Vorgang als abgeschlossen markiert und es können zukünftig weitere Kryptogramme bestellt werden.
4. Gültiges One Time Password (OTP) und die zu dem OTP-Token gehörige PIN eingeben
5. Klicken auf Schaltfläche „Alle Bestätigen“



Abbildung 12: Bestätigen von Kryptogrammen (beispielhaft)



Weiterführende Dokumentation: siehe [Bedienungsanleitung KM-Web-Service](#) ab S.20 ff.

Abbildungsverzeichnis

- *Abbildung 1* Bestätigen von Kryptogrammen (beispielhaft) S. 5
- *Abbildung 2* Anlegen einer SAM-Gruppe, Typ „SAM-Art“ S. 6
- *Abbildung 3* Anlegen einer SAM-Gruppe, Typ „SAM-Art“ S. 8
- – Gültigkeitsbereich I
- *Abbildung 4* Anlegen einer SAM-Gruppe, Typ „SAM-Art“ S. 9
- – Gültigkeitsbereich II
- *Abbildung 5* Anlegen einer SAM-Gruppe, Typ „SAM-Art“ S. 10
- – Gültigkeitsbereich III
- *Abbildung 6* Kryptogrammauftrag, Schlüssel auswählen und hinzufügen S. 11
- *Abbildung 7* Kryptogrammauftrag, Schlüssel auswählen und hinzufügen S. 12
- *Abbildung 8* alle Kryptogramme als Paket herunterladen (Option a) S. 13
- *Abbildung 9* Speichern der Kryptogramme S. 14
- *Abbildung 10* Gespeicherte Kryptogramme als ZIP-Datei S. 15
- *Abbildung 11* Inhalt Downloaddateien S. 16
- *Abbildung 12* Bestätigen von Kryptogrammen (beispielhaft) S. 17