



A **Global Payments** Company

# Production Certification Authority Public Keys

# TABLE OF CONTENTS

|  |   |
|--|---|
| Summary of Changes                             | 4 |
| Introduction                                   | 5 |
| Intent of Document                             | 5 |
| Intended Audience                              | 5 |
| Disclosure                                     | 5 |
| Key Management Requirements                    | 5 |
| Introduction                                   | 5 |
| Certification Authority Public Key Storage     | 5 |
| Certification Authority Public Key Storage     | 7 |
| Production Certification Authority Public Keys | 7 |

## **Copyright**

This document is proprietary to TSYS and has been furnished on a confidential and restricted basis. This document details TSYS' capabilities. These elements are essential to TSYS' business and are proprietary.

TSYS is providing this document with the express understanding that it will be held in confidence. Any reproduction, use, or display or other disclosure or dissemination, by any method now known or later developed, of this material or the information contained herein, in whole or in part, without the prior written consent of Global Payments is strictly prohibited.

TSYS logo is registered trademark of TSYS and may not be copied, imitated or used, in whole or in part, without prior written permission. All other trademarks, registered trademarks, product names, and logos identified or mentioned herein are the property of their respective owners.

## **Disclaimer**

Information provided herein is limited by the capabilities in existence at the time the document was created, as well as by information made available by the Card Associations, EMVCo, and the Debit Networks. The information contained herein is advisory in nature. TSYS makes no warranties, express or implied, as to any services, software or documentation. TSYS specifically disclaims any and all implied warranties, including without limitation any implied warranties of merchantability, fitness for a particular purpose, title, non-infringement of third-party rights, or any warranties arising from a course of dealing, usage or trade practice.

## **License**

Ownership all TSYS documents, related documentation and all intellectual property rights herein and hereto shall remain at all times with TSYS. All rights not expressly granted herein are reserved to TSYS. TSYS grants authorized recipients of this document the limited right to use it and its contents for informational purposes intended to facilitate the transmission of transactions to the TSYS Hosts, and for no other purpose.

## Summary of Changes

| Date       | Summary                               |
|------------|---------------------------------------|
| 01/11/2021 | Initial creation of combined document |
|            |                                       |
|            |                                       |
|            |                                       |
|            |                                       |
|            |                                       |
|            |                                       |
|            |                                       |
|            |                                       |
|            |                                       |

## ***Intent of Document***

TSYS' Production CAPK document provides the CAPK keys needed to run EMV production transactions. This document will be stored on the Developer Portal.

## ***Intended Audience***

This document is intended for POS developers who have successfully run transaction in certification and need to run a Production Test and Production Transactions.

## ***Disclosure***

This Guide reflects Global Payments' interpretations of the Brand, Network and EMVCo requirements and specifications. Readers of this document should continue to refer to and review all EMVCo documentation and obtain advice from their own legal and technical personnel.

## ***Key Management Requirements***

### **Introduction**

The following principles apply to the introduction of a Certification Authority Public Key from an acquirer to its terminals:

- The terminal shall be able to verify that it received the Certification Authority Public Key and its related data error free from the acquirer
- The terminal shall be able to verify that the received Certification Authority Public Key and related data originated from its legitimate acquirer

### **Certification Authority Public Key Storage**

**As specified in the EMV4.3 - Book 2 specification document:**

- Terminals that support offline static or dynamic data authentication shall provide support for six Certification Authority Public Keys per RID for EMVCo member debit/credit applications based on the EMVCo Book 2 specification
- Each Certification Authority Public Key is **uniquely identified by the 5-byte RID** that identifies the payment system in question, and the 1-byte Certification Authority Public Key Index, unique per RID and assigned by that payment system to a particular Certification Authority Public Key
- For each Certification Authority Public Key, the minimum set of data elements that shall be available in the terminal is specified in Table 27 of the EMVCo Book 2 specification
- The RID and the Certification Public Key Index together uniquely identify the Certification Authority Public Key and associate it with the proper payment system
- The Certification Authority Public Key Algorithm Indicator identifies the digital signature algorithm to be used with the corresponding Certification Authority Public Key. The only acceptable value at this moment is hexadecimal '01', indicating the usage of the RSA algorithm in the digital signature scheme as specified in the EMVCo Book 2 specification Annex A2.1 and Annex B2.1. The Hash Algorithm Indicator specifies the hashing algorithm to produce the Hash Result in the digital signature scheme. The only acceptable value at this moment is hexadecimal '01', indicating the usage of the SHA-1 algorithm

- The Certification Authority Public Key Check Sum is derived using the technique specified in section 10.2 of the EMVCo Book 4, to ensure that a Certification Authority Public Key and its related data are received error-free. The terminal may use this data element to subsequently re-verify the integrity of a Certification Authority Public Key and its related data. Alternately, the terminal may use another technique to ensure the integrity of this data
- The integrity of the stored Certification Authority Public Keys should be verified periodically

Table 27: Minimum Set of Certification Authority Public Key Related Data Elements to be Stored in Terminal

| Field Name   | Length         | Description   | Format |
|--|----------------|---|--------|
| Registered Application Provider Identifier (RID)       | 5              | Identifies the payment system to which the Certification Authority Public Key is associated   | b      |
| Certification Authority Public Key Index               | 1              | Identifies the Certification Authority Public Key in conjunction with the RID   | b      |
| Certification Authority Hash Algorithm Indicator       | 1              | Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme   | b      |
| Certification Authority Public Key Algorithm Indicator | 1              | Identifies the digital signature algorithm to be used with the Certification Authority Public Key   | b      |
| Certification Authority Public Key Modulus             | Var. (max 248) | Value of the modulus part of the Certification Authority Public Key   | b      |
| Certification Authority Public Key Exponent            | 1 or 3         | Value of the exponent part of the Certification Authority Public Key, equal to 3 or $2^{16} + 1$  | b      |
| Certification Authority Public Key Check Sum 40        | 20             | A check value calculated on the concatenation of all parts of the Certification Authority Public Key (RID, Certification Authority Public Key Index, Certification Authority Public Key Modulus, Certification Authority Public Key Exponent) using SHA-1 | b      |

## Certification Authority Public Key Storage

The following principles apply for the withdrawal of Certification Authority Public Keys from its terminals:

- The terminal shall be able to verify that it received the withdrawal notification error free remotely
- The terminal shall be able to verify that the received withdrawal notification originated from its legitimate acquirer
- The acquirer shall be able to confirm that a specific Certification Authority Public Key was indeed withdrawn correctly from its terminals

## Production Certification Authority Public Keys

The following Certification Authority Public Keys (CAPKs) need to be in your applications for Production transactions. We recommend that you do not store the expiration date in your software/application, but provide them for reference.

| RID                          | Index | CA Public Key Modulus   | Public Key Exponent | Hash  | Expiration Date |
|------------------------------|-------|---|---------------------|---|-----------------|
| A0 00 00 00 04<br>Mastercard | 05    | (1408 bits)<br>B8 04 8A BC 30 C9 0D 97 63 36 54 3E 3F D7<br>09 1C 8F E4 80 0D F8 20 ED 55 E7 E9 48 13<br>ED 00 55 5B 57 3F EC A3 D8 4A F6 13 1A 65<br>1D 66 CF F4 28 4F B1 3B 63 5E DD 0E E4 01<br>76 D8 BF 04 B7 FD 1C 7B AC F9 AC 73 27 DF<br>AA 8A A7 2D 10 DB 3B 8E 70 B2 DD D8 11 CB<br>41 96 52 5E A3 86 AC C3 3C 0D 9D 45 75 91<br>64 69 C4 E4 F5 3E 8E 1C 91 2C C6 18 CB 22<br>DD E7 C3 56 8E 90 02 2E 6B BA 77 02 02 E4<br>52 2A 2D D6 23 D1 80 E2 15 BD 1D 15 07 FE<br>3D C9 0C A3 10 D2 7B 3E FC CD 8F 83 DE 30<br>52 CA D1 E4 89 38 C6 8D 09 5A AC 91 B5 F3<br>7E 28 BB 49 EC 7E D5 97  | 3                   | (20 bytes)<br>EB FA 0D 5D 06 D8 CE<br>70 2D A3 EA E8 90 70<br>1D 45 E2 74 C8 45 | 31 Dec 2024     |
| A0 00 00 00 04<br>Mastercard | 06    | (1984 bits)<br>CB 26 FC 83 0B 43 78 5B 2B CE 37 C8 1E D3<br>34 62 2F 96 22 F4 C8 9A AE 64 10 46 B2 35<br>34 33 88 3F 30 7F B7 C9 74 16 2D A7 2F 7A<br>4E C7 5D 9D 65 73 36 86 5B 8D 30 23 D3 D6<br>45 66 76 25 C9 A0 7A 6B 7A 13 7C F0 C6 41<br>98 AE 38 FC 23 80 06 FB 26 03 F4 1F 4F 3B<br>B9 DA 13 47 27 0F 2F 5D 8C 60 6E 42 09 58<br>C5 F7 D5 0A 71 DE 30 14 2F 70 DE 46 88 89<br>B5 E3 A0 86 95 B9 38 A5 0F C9 80 39 3A 9C<br>BC E4 4A D2 D6 4F 63 0B B3 3A D3 F5 F5 FD<br>49 5D 31 F3 78 18 C1 D9 40 71 34 2E 07 F1<br>BE C2 19 4F 60 35 BA 5D ED 39 36 50 0E B8<br>2D FD A6 E8 AF B6 55 B1 EF 3D 0D 7E BF 86<br>B6 6D D9 F2 9F 6B 1D 32 4F E8 B2 6C E3 8A<br>B2 01 3D D1 3F 61 1E 7A 59 4D 67 5C 44 32<br>35 0E A2 44 CC 34 F3 87 3C BA 06 59 29 87<br>A1 D7 E8 52 AD C2 2E F5 A2 EE 28 13 20 31<br>E4 8F 74 03 7E 3B 34 AB 74 7F | 3                   | (20 bytes)<br>F9 10 A1 50 4D 5F FB<br>79 3D 94 F3 B5 00 76<br>5E 1A BC AD 72 D9 | 31 Dec 2029     |

| RID                                   | Index | CA Public Key Modulus   | Public Key Exponent | Hash  | Expiration Date |
|---------------------------------------|-------|---|---------------------|---|-----------------|
| A0 00 00 00 03<br>VISA                | 08    | (1408 bits)<br>D9 FD 6E D7 5D 51 D0 E3 06 64 BD 15 70 23<br>EA A1 FF A8 71 E4 DA 65 67 2B 86 3D 25 5E<br>81 E1 37 A5 1D E4 F7 2B CC 9E 44 AC E1 21<br>27 F8 7E 26 3D 3A F9 DD 9C F3 5C A4 A7 B0<br>1E 90 70 00 BA 85 D2 49 54 C2 FC A3 07 48<br>25 DD D4 C0 C8 F1 86 CB 02 0F 68 3E 02 F2<br>DE AD 39 69 13 3F 06 F7 84 51 66 AC EB 57<br>CA 0F C2 60 34 45 46 98 11 D2 93 BF EF BA<br>FA B5 76 31 B3 DD 91 E7 96 BF 85 0A 25 01<br>2F 1A E3 8F 05 AA 5C 4D 6D 03 B1 DC 2E 56<br>86 12 78 59 38 BB C9 B3 CD 3A 91 0C 1D A5<br>5A 5A 92 18 AC E0 F7 A2 12 87 75 26 82 F1<br>58 32 A6 78 D6 E1 ED 0B  | 3                   | (20 bytes)<br>20 D2 13 12 69 55 DE<br>20 5A DC 2F D2 82 2B<br>D2 2D E2 1C F9 A8 | 31 Dec 2024     |
| A0 00 00 00 03<br>VISA                | 09    | (1984 bits)<br>9D 91 22 48 DE 0A 4E 39 C1 A7 DD E3 F6 D2<br>58 89 92 C1 A4 09 5A FB D1 82 4D 1B A7 48<br>47 F2 BC 49 26 D2 EF D9 04 B4 B5 49 54 CD<br>18 9A 54 C5 D1 17 96 54 F8 F9 B0 D2 AB 5F<br>03 57 EB 64 2F ED A9 5D 39 12 C6 57 69 45<br>FA B8 97 E7 06 2C AA 44 A4 AA 06 B8 FE 6E<br>3D BA 18 AF 6A E3 73 8E 30 42 9E E9 BE 03<br>42 7C 9D 64 F6 95 FA 8C AB 4B FE 37 68 53<br>EA 34 AD 1D 76 BF CA D1 59 08 C0 77 FF E6<br>DC 55 21 EC EF 5D 27 8A 96 E2 6F 57 35 9F<br>FA ED A1 94 34 B9 37 F1 AD 99 9D C5 C4 1E<br>B1 19 35 B4 4C 18 10 0E 85 7F 43 1A 4A 5A<br>6B B6 51 14 F1 74 C2 D7 B5 9F DF 23 7D 6B<br>B1 DD 09 16 E6 44 D7 09 DE D5 64 81 47 7C<br>75 D9 5C DD 68 25 46 15 F7 74 0E C0 7F 33<br>0A C5 D6 7B CD 75 BF 23 D2 8A 14 08 26 C0<br>26 DB DE 97 1A 37 CD 3E F9 B8 DF 64 4A C3<br>85 01 05 01 EF C6 50 9D 7A 41 | 3                   | (20 bytes)<br>1F F8 0A 40 17 3F 52<br>D7 D2 7E 0F 26 A1 46<br>A1 C8 CC B2 90 46 | 31 Dec 2029     |
| A0 00 00 00 25<br>American<br>Express | 0F    | (1408 bits)<br>C8 D5 AC 27 A5 E1 FB 89 97 8C 7C 64 79 AF<br>99 3A B3 80 0E B2 43 99 6F BB 2A E2 6B 67<br>B2 3A C4 82 C4 B7 46 00 5A 51 AF A7 D2 D8<br>3E 89 4F 59 1A 23 57 B3 0F 85 B8 56 27 FF<br>15 DA 12 29 0F 70 F0 57 66 55 2B A1 1A D3<br>4B 71 09 FA 49 DE 29 DC B0 10 96 70 87 5A<br>17 EA 95 54 9E 92 34 7B 94 8A A1 F0 45 75<br>6D E5 6B 70 7E 38 63 E5 9A 6C BE 99 C1 27<br>2E F6 5F B6 6C BB 4C FF 07 0F 36 02 9D D7<br>62 18 B2 12 42 64 5B 51 CA 75 2A F3 7E 70<br>BE 1A 84 FF 31 07 9D C0 04 8E 92 88 83 EC<br>4F AD D4 97 A7 19 38 5C 2B BB EB C5 A6 6A<br>A5 E5 65 5D 18 03 4E C5  | 3                   | (20 bytes)<br>A7 34 72 B3 AB 55 74<br>93 A9 BC 21 79 CC 80<br>14 05 3B 12 BA B4 | 31 Dec 2024     |



| RID                                | Index | CA Public Key Modulus   | Public Key Exponent | Hash  | Expiration Date |
|------------------------------------|-------|---|---------------------|---|-----------------|
| A0 00 00 00 25<br>American Express | 10    | (1984 bits)<br>CF 98 DF ED B3 D3 72 79 65 EE 77 97 72 33<br>55 E0 75 1C 81 D2 D3 DF 4D 18 EB AB 9F B9<br>D4 9F 38 C8 C4 A8 26 B9 9D C9 DE A3 F0 10<br>43 D4 BF 22 AC 35 50 E2 96 2A 59 63 9B 13<br>32 15 64 22 F7 88 B9 C1 6D 40 13 5E FD 1B<br>A9 41 47 75 05 75 E6 36 B6 EB C6 18 73 4C<br>91 C1 D1 BF 3E DC 2A 46 A4 39 01 66 8E 0F<br>FC 13 67 74 08 0E 88 80 44 F6 A1 E6 5D C9<br>AA A8 92 8D AC BE B0 DB 55 EA 35 14 68 6C<br>6A 73 2C EF 55 EE 27 CF 87 7F 11 06 52 69<br>4A 0E 34 84 C8 55 D8 82 AE 19 16 74 E2 5C<br>29 62 05 BB B5 99 45 51 76 FD D7 BB C5 49<br>F2 7B A5 FE 35 33 6F 7E 29 E6 8D 78 39 73<br>19 94 36 63 3C 67 EE 5A 68 0F 05 16 0E D1<br>2D 16 65 EC 83 D1 99 7F 10 FD 05 BB DB F9<br>43 3E 8F 79 7A EE 3E 9F 02 A3 42 28 AC E9<br>27 AB E6 2B 8B 92 81 AD 08 D3 DF 5C 73 79<br>68 50 45 D7 BA 5F CD E5 86 37 | 3                   | (20 bytes)<br>C7 29 CF 2F D2 62 39<br>4A BC 4C C1 73 50 65<br>02 44 6A A9 B9 FD | 31 Dec 2029     |
| A0 00 00 01 52<br>Discover Network | 4     | (1408 bits)<br>8E EE C0 D6 D3 85 7F D5 58 28 5E 49 B6 23<br>B1 09 E6 77 4E 06 E9 47 6F E1 B2 FB 27 36<br>85 B5 A2 35 E9 55 81 0A DD B5 CD CC 2C B6<br>E1 A9 7A 07 08 9D 7F DE 0A 54 8B DC 62 21<br>45 CA 2D E3 C7 3D 6B 14 F2 84 B3 DC 1F A0<br>56 FC 0F B2 81 8B CD 7C 85 2F 0C 97 96 31<br>69 F0 14 83 CE 1A 63 F0 BF 89 9D 41 2A B6<br>7C 5B BD C8 B4 F6 FB 9A BB 57 E9 51 25 36<br>3D BD 8F 5E BA A9 B7 4A DB 93 20 20 50 34<br>18 33 DE E8 E3 8D 28 BD 17 5C 83 A6 EA 72<br>0C 26 26 82 BE AB EA 8E 95 5F E6 7B D9 C2<br>EF F7 CB 9A 9F 45 DD 5B DA 4A 1E EF B1 48<br>BC 44 FF F6 8D 93 29 FD  | 3                   | (20 bytes)<br>17 F9 71 CA F6 B7 08<br>E5 B9 16 53 31 FB A9<br>15 93 D0 C0 BF 66 | 31 Dec 2024     |
| A0 00 00 01 52<br>Discover Network | 5     | (1984 bits)<br>E1 20 0E 9F 44 28 EB 71 A5 26 D6 BB 44 C9<br>57 F1 8F 27 B2 0B AC E9 78 06 1C CE F2 35<br>32 DB EB FA F6 54 A1 49 70 1C 14 E6 A2 A7<br>C2 EC AC 4C 92 13 5B E3 E9 25 83 31 DD B0<br>96 7C 3D 1D 37 5B 99 6F 25 B7 78 11 CC CC<br>06 A1 53 B4 CE 69 90 A5 1A 02 58 EA 84 37<br>ED BE B7 01 CB 1F 33 59 93 E3 F4 84 58 BC<br>11 94 BA D2 9B F6 83 D5 F3 EC B9 84 E3 1B<br>7B 9D 2F 6D 94 7B 39 DE DE 02 79 EE 45 B4<br>7F 2F 3D 4E EE F9 3F 92 61 F8 F5 A5 71 AF BF<br>B5 69 C1 50 37 0A 78 F6 68 3D 68 7C B6 77<br>77 7B 2E 7A BE FC FC 8F 5F 93 50 17 36 99<br>7E 83 10 EE 0F D8 7A FA C5 DA 77 2B A2 77<br>F8 8B 44 45 9F CA 56 35 55 01 7C D0 D6 67<br>71 43 7F 8B 66 08 AA 1A 66 5F 88 D8 46 40<br>3E 4C 41 AF EE DB 97 29 C2 B2 51 1C FE 22<br>8B 50 C1 B1 52 B2 A6 0B BF 61 D8 91 3E 08<br>62 10 02 3A 3A A4 99 E4 23 | 3                   | (20 bytes)<br>12 BC D4 07 B6 E6 27<br>A7 50 FD F6 29 EE 8C<br>2C 9C C7 BA 63 6A | 31 Dec 2026     |

| RID                   | Index | CA Public Key Modulus   | Public Key Exponent | Hash  | Expiration Date |
|-----------------------|-------|---|---------------------|---|-----------------|
| A0 00 00 00 65<br>JCB | 12    | (1408 bits)<br>AD F0 5C D4 C5 B4 90 B0 87 C3 46 7B 0F 30<br>43 75 04 38 84 84 61 28 8B FE FD 61 98 DD<br>57 6D C3 AD 7A 7C FA 07 DB A1 28 C2 47 A8<br>EA B3 0D C3 A3 0B 02 FC D7 F1 C8 16 79 65<br>46 36 26 FE FF 8A B1 AA 61 A4 B9 AE F0 9E<br>E1 2B 00 98 42 A1 AB A0 1A DB 4A 2B 17 06<br>68 78 1E C9 2B 60 F6 05 FD 12 B2 B2 A6 F1<br>FE 73 4B E5 10 F6 0D C5 D1 89 E4 01 45 1B<br>62 B4 E0 68 51 EC 20 EB FF 45 22 AA CC 2E<br>9C DC 89 BC 5D 8C DE 5D 63 3C FD 77 22 0F<br>F6 BB D4 A9 B4 41 47 3C C3 C6 FE FC 8D 13<br>E5 7C 3D E9 7E 12 69 FA 19 F6 55 21 5B 23<br>56 3E D1 D1 86 0D 86 81  | 3                   | (20 bytes)<br>87 4B 37 9B 7F 60 7D<br>C1 CA F8 7A 19 E4 00<br>B6 A9 E2 51 63 E8 | 31 Dec 2024     |
| A0 00 00 00 65<br>JCB | 14    | (1984 bits)<br>AE ED 55 B9 EE 00 E1 EC EB 04 5F 61 D2 DA<br>9A 66 AB 63 7B 43 FB 5C DB DB 22 A2 FB B2<br>5B E0 61 E9 37 E3 82 44 EE 51 32 F5 30 14<br>4A 3F 26 89 07 D8 FD 64 88 63 F5 A9 6F ED<br>7E 42 08 9E 93 45 7A DC 0E 1B C8 9C 58 A0<br>DB 72 67 5F BC 47 FE E9 FF 33 C1 6A DE 6D<br>34 19 36 B0 6B 6A 6F 5E F6 F6 6A 4E DD 98<br>1D F7 5D A8 39 9C 30 53 F4 30 EC A3 42 43<br>7C 23 AF 42 3A 21 1A C9 F5 8E AF 09 B0 F8<br>37 DE 9D 86 C7 10 9D B1 64 65 61 AA 5A F0<br>28 9A F5 51 4A C6 4B C2 D9 D3 6A 17 9B B8<br>A7 97 1E 2B FA 03 A9 E4 B8 47 FD 3D 63 52<br>4D 43 A0 E8 00 35 47 B9 4A 8A 75 E5 19 DF<br>31 77 D0 A6 0B C0 B4 BA B1 EA 59 A2 CB B4<br>D2 D6 23 54 E9 26 E9 C7 D3 BE 41 81 E8 1B<br>A6 0F 82 85 A8 96 D1 7D A8 C3 24 24 81 B6<br>C4 05 76 9A 39 D5 47 C7 4E D9 FF 95 A7 0A<br>79 60 46 B5 EF F3 66 82 DC 29 | 3                   | (20 bytes)<br>C0 D1 5F 6C D9 57 E4<br>91 DB 56 DC DD 1C A8<br>7A 03 EB E0 6B 7B | 31 Dec 2030     |
| A000000333<br>UCIS    | 02    | (1152 bits)<br>A3 76 7A BD 1B 6A A6 9D 7F 3F BF 28 C0 92<br>DE 9E D1 E6 58 BA 5F 09 09 AF 7A 1C CD 90<br>73 73 B7 21 0F DE B1 62 87 BA 8E 78 E1 52<br>9F 44 39 76 FD 27 F9 91 EC 67 D9 5E 5F 4E<br>96 B1 27 CA B2 39 6A 94 D6 E4 5C DA 44 CA<br>4C 48 67 57 0D 6B 07 54 2F 8D 4B F9 FF 97<br>97 5D B9 89 15 15 E6 6F 52 5D 2B 3C BE B6<br>D6 62 BF B6 C3 F3 38 E9 3B 02 14 2B FC 44<br>17 3A 37 64 C5 6A AD D2 02 07 5B 26 DC 2F<br>9F 7D 7A E7 4B D7 D0 0F D0 5E E4 30 03 26<br>63 D2 7A 57  | 3                   | (20 bytes)<br>03 BB 33 5A 85 49 A0<br>3B 87 AB 08 9D 00 6F<br>60 85 2E 4B 80 60 | 31 Dec 2021     |

| RID                | Index | CA Public Key Modulus   | Public Key Exponent | Hash  | Expiration Date |
|--------------------|-------|---|---------------------|---|-----------------|
| A000000333<br>UCIS | 03    | (1408 bits)<br>B0 62 7D EE 87 86 4F 9C 18 C1 3B 9A 1F 02<br>54 48 BF 13 C5 83 80 C9 1F 4C EB A9 F9 BC<br>B2 14 FF 84 14 E9 B5 9D 6A BA 10 F9 41 C7<br>33 17 68 F4 7B 21 27 90 7D 85 7F A3 9A AF<br>8C E0 20 45 DD 01 61 9D 68 9E E7 31 C5 51<br>15 9B E7 EB 2D 51 A3 72 FF 56 B5 56 E5 CB<br>2F DE 36 E2 30 73 A4 4C A2 15 D6 C2 6C A6<br>88 47 B3 88 E3 95 20 E0 02 6E 62 29 4B 55<br>7D 64 70 44 0C A0 AE FC 94 38 C9 23 AE C9<br>B2 09 8D 6D 3A 1A F5 E8 B1 DE 36 F4 B5 30<br>40 10 9D 89 B7 7C AF AF 70 C2 6C 60 1A BD<br>F5 9E EC 0F DC 8A 99 08 91 40 CD 2E 81 7E<br>33 51 75 B0 3B 7A A3 3D  | 3                   | (20 bytes)<br>87 F0 CD 7C 0E 86 F3<br>8F 89 A6 6F 8C 47 07<br>1A 8B 88 58 6F 26 | 31 Dec 2024     |
| A000000333<br>UCIS | 04    | (1984 bits)<br>BC 85 3E 6B 53 65 E8 9E 7E E9 31 7C 94 B0<br>2D 0A BB 0D BD 91 C0 5A 22 4A 25 54 AA 29<br>ED 9F CB 9D 86 EB 9C CB B3 22 A5 78 11 F8<br>61 88 AA C7 35 1C 72 BD 9E F1 96 C5 A0 1A<br>CE F7 A4 EB 0D 2A D6 3D 9E 6A C2 E7 83 65<br>47 CB 15 95 C6 8B CB AF D0 F6 72 87 60 F3<br>A7 CA 7B 97 30 1B 7E 02 20 18 4E FC 4F 65<br>30 08 D9 3C E0 98 C0 D9 3B 45 20 10 96 D1<br>AD FF 4C F1 F9 FC 02 AF 75 9D A2 7C D6 DF<br>D6 D7 89 B0 99 F1 6F 37 8B 61 00 33 4E 63<br>F3 D3 5F 32 51 A5 EC 78 69 37 31 F5 23 35<br>19 CD B3 80 F5 AB 8C 0F 02 72 8E 91 D4 69<br>AB D0 EA E0 D9 3B 1C C6 6C E1 27 B2 9C 7D<br>77 44 1A 49 D0 9F CA 5D 6D 97 62 FC 74 C3<br>1B B5 06 C8 BA E3 C7 9A D6 C2 57 87 75 B9<br>59 56 B5 37 0D 1D 05 19 E3 79 06 B3 84 73<br>62 33 25 1E 8F 09 AD 79 DF BE 2C 6A BF AD<br>AC 8E 4D 86 24 31 8C 27 DA F1 | 3                   | (20 bytes)<br>F5 27 08 1C F3 71 DD<br>7E 1F D4 FA 41 4A 66<br>50 36 E0 F5 E6 E5 | 31 Dec 2031     |