

Buletin ASPI
No: 4/CERT/VII/2021

NSICCS Certificate Authority Public Key – Juli 2021

Pendahuluan

Berdasarkan Peraturan Bank Indonesia nomor 19/8/PBI/2017 tanggal 6 Juli 2017 tentang Gerbang Pembayaran Nasional (*National Payment Gateway*) disebutkan bahwa salah satu tugas ASPI sebagai Lembaga Standar adalah mengelola dan melaksanakan *Key Management* sebagai *Certificate Authority* (CA) untuk Standar Nasional Teknologi *Chip* NSICCS yang telah ditetapkan sebagai standar nasional untuk kartu ATM dan/atau Debet. Dalam menjalankan fungsi key management/CA, ASPI menerbitkan sertifikat untuk *Issuer* atau *Issuer Public Key Certificate* (IPKC) dan mengelola kunci digital (*key*) dalam rangka menjaga keamanan transmisi data suatu transaksi pembayaran.

Sehubungan dengan hal tersebut diatas, ASPI telah menyediakan NSICCS CA Public Key 1984-bit sesuai dengan buletin yang dikeluarkan oleh EMV pada bulan Juli 2020 yang merekomendasikan penggunaan public key 1984-bit dengan masa berlaku hingga akhir Desember 2030. Mengingat bahwa Standar Nasional Teknologi *Chip* NSICCS mengacu pada spesifikasi EMV, maka ASPI mengikuti rekomendasi tersebut dengan menerapkan *NSICCS Certificate Authority Public Key* ("*NSICCS CA Public Key*") 1984-bit mulai 2 Agustus 2021.

Dengan telah diterapkannya *NSICCS CA Public Key* 1984-bit maka pelaku sistem pembayaran yang terlibat dalam pemrosesan transaksi yang menggunakan Standar NSICCS Teknologi *Chip* pada kartu ATM dan/atau Debet harus melakukan penyesuaian terhadap sistem dan perangkatnya.

Dibawah ini penyesuaian yang diperlukan:

A. Acquirer

- Mulai tanggal 1 September 2021, setiap terminal NSICCS non-ATM **baru** yang disediakan/dipasang oleh Acquirer wajib sudah mengimplementasikan 2 (dua) *Public Key production* yaitu *NSICCS CA Public Key* 1984-bit dan *NSICCS CA Public Key* 1408-bit – *Production*.
 - Mulai tanggal 1 Januari 2022, **semua** terminal NSICCS non-ATM wajib sudah dapat memproses transaksi menggunakan *NSICCS CA Public Key* 1984-bit dan 1408-bit.
 - Hanya *NSICCS CA Public Key* 1984-bit dan *NSICCS CA Public Key* 1408-bit - *Production* yang harus digunakan pada terminal yang beredar.
 - *NSICCS CA Public Key - Test* tidak diperkenankan untuk digunakan pada terminal yang beredar.
-

B. Penerbit

- Semua Penerbit perlu melakukan penyesuaian pada sistem personalisasi kartu sehubungan dengan penerbitan kartu yang menggunakan *NSICCS CA Public Key* 1984-bit.
- Mulai tanggal 1 Januari 2022, penerbit dapat mengeluarkan kartu NSICCS yang menggunakan *NSICCS CA Public Key* 1984-bit dengan masa berlaku hingga 31 Desember 2030.

C. Functional Laboratory

- Lab fungsional wajib melakukan penyesuaian pada perangkat pengujian (*test tools*) untuk memastikan pengujian dengan menggunakan *NSICCS CA Public Key* 1984-bit dapat dilaksanakan dengan baik mulai tanggal 1 Oktober 2021.
- Pengujian yang dilakukan meliputi, namun tidak terbatas pada:
 - o kartu ATM dan/atau kartu Debet berteknologi *chip* yang menggunakan standar NSICCS
 - o terminal non-ATM berteknologi *chip* yang menggunakan standar NSICCS
 - o CPT berteknologi *chip* yang menggunakan standar NSICCS

D. Biro Personalisasi

- Wajib melakukan penyesuaian sistem dan hal lain yang diperlukan agar dapat memproses personalisasi kartu yang menggunakan *NSICCS CA Public Key* 1984-bit mulai tanggal 1 Januari 2022.

E. Pelaporan

Semua pihak yang telah melakukan penyesuaian wajib melaporkan kepada ASPI selambat-lambatnya 1 bulan setelah penyesuaian.

1. NSICCS CA PUBLIC KEY – PRODUCTION

Dibawah ini *NSICCS Certificate Authority Public Key length* yang berlaku beserta tanggal jatuh tempo dari masing-masing kunci tersebut.

NSICCS CA Public Key

Key	Masa berlaku (<i>expiration date</i>)	Keterangan
1408-bit	31 Desember 2026	Maksimum masa berlaku untuk <i>Issuer Public Key Certificate</i> adalah 31 Desember 2026
1984-bit	31 Desember 2030	Mulai tanggal 1 Januari 2022 semua terminal NSICCS non-ATM sudah memasukan (load) <i>NSICCS CA Public Key</i> 1984-bit. Maksimum masa berlaku untuk <i>Issuer Public Key Certificate</i> adalah 31 Desember 2030

1.1 NSICCS CA Public Key 1408 bit - Production

Komponen (<i>component</i>)	Nilai (<i>value</i>)
Registered Application Provider Identifier (RID)	A0 00 00 06 02
Index	05
Modulus	B4 8C C6 3D 71 A4 86 DF C9 20 60 8A 3E 42 D7 C3 05 47 2B F7 6B 8E 50 C8 C0 2F B8 38 7E 78 8F 72 93 1A 29 DC 15 F9 13 E7 D6 9E 43 AD 4C 38 A5 C4 31 7E 36 D1 5D E5 F4 9F A2 32 7D 97 54 79 9D 24 84 A6 E1 56 94 1A CA 96 32 41 7E 5C 92 93 1A 85 E1 BB 5F 2A 2C 1B 84 7D 50 08 C7 B3 05 91 F1 AC BF 3B 98 DF B0 CF 28 49 B6 C7 CD C7 43 5A EA 85 F3 A5 8B AC 3B 8C 99 04 16 A5 E1 9E C4 EA 08 DC 91 CE F2 FB E5 94 0F A6 62 29 26 D2 AD 05 23 D1 09 A7 02 4E B1 03 5B BE 37 26 0B 30 F4 1A A5 2E EB 36 E6 0D D3 71 20 B9 40 1C 38 50 92 0F 0E 03
Exponent	03
Secure Hash Algorithm – 1 Hash	1C AB 16 2A 1B E8 14 92 BB 95 2C 28 46 61 7B 75 6F 83 3C 07

1.2 NSICCS CA Public Key 1984 bit – Production

Komponen (component)	Nilai (value)
Registered Application Provider Identifier (RID)	A0 00 00 06 02
Index	09
Modulus	A5 17 A3 38 85 4E 08 56 EE 4A FD BF 4B DA 5D D3 F9 EB 38 95 CB D8 97 1B 1E 58 A8 EB 16 7B F9 93 5E 07 52 DA EA 7E AF B2 5E 79 D6 01 EB 20 18 95 A9 3F 8B 0A 16 D9 5A 23 03 66 C0 5F EC 55 85 8C 94 D6 09 7B 2F B1 ED DD 2C 6A 36 47 DD 0B 71 BC 1D CD DC 68 B4 E9 EC C9 19 FB 54 40 70 95 24 43 15 97 33 47 12 92 99 3A B2 3E 5B 8C 00 E6 A8 52 6D F0 4A 0B 6E 65 E0 F9 D0 37 8F 71 49 7E 12 FA 83 54 0B 49 FC 05 D0 A8 6D C3 D6 6F C4 BB 29 1A 69 B2 EB B9 8D 05 7C 8F 1E E7 CB 8E 94 2F D0 5E 9E 4F AD 03 61 BC 18 4C 13 41 8C 31 3C 04 2C 54 7D EF 41 31 0B A1 85 0E F5 9C AF 8C C7 B1 4D AE E7 2F A4 68 9C 10 47 43 40 24 D5 65 A3 FA 46 ED CA 3F 53 E2 36 23 52 68 C8 93 F2 68 AA 24 AB 2D 20 EB 7A E0 6F F3 12 33 18 04 1C B2 3E 30 83 9C 58 DF D4 99 1D 7C 88 CB
Exponent	03
Secure Hash Algorithm – 1 Hash	E7 86 86 DB 11 9C 1C BF AD 21 49 EF 3C BE 9C F5 4A C6 32 1E

2. NSICCS CA PUBLIC KEY – TEST

2.1 NSICCS CA Public Key 1408 bit - Test

Komponen (component)	Nilai (value)
Registered Application Provider Identifier (RID)	A0 00 00 06 02
Index	F5
Modulus	9F 2E 97 2F F3 F0 07 59 77 2A F8 50 CB CD 0B 8B E4 11 FE 2D 10 4C EB 1B 21 8E 91 F9 F0 08 DC C3 0D E6 1F 42 22 4C 6A 6B E0 7D AC 04 8D A1 6C F2 4C 43 E6 00 CE C4 BB D4 C5 67 44 94 78 8F 70 3A A4 46 9E 7D BC 3B 99 23 C2 C5 4B 50 D4 97 1D 17 6A 0E 62 F6 87 56 11 B9 CE 5E 24 7D 24 AC 26 92 6F 22 D0 70 5D 39 A6 58 08 79 02 32 70 2E 8C 1A 80 29 1C A2 C8 AD 89 09 25 B0 EA 20 06 97 61 DF 86 3B 37 4F FB 41 A5 3E CB 22 98 67 FB C6 47 5C 05 4B 40 7C 41 E1 70 26 5F 08 63 4E 61 32 42 28 A3 24 66 EF 26 E6 BD 5A 2C 15 07 40 A2 F5 D7 B5
Exponent	03
Secure Hash Algorithm – 1 Hash	72 45 4E B3 8A 36 0F B9 73 59 63 E8 A1 7E 82 56 C9 28 16 DB

2.2 NSICCS CA Public Key 1984 bit – Test

Komponen (<i>component</i>)	Nilai (<i>value</i>)
Registered Application Provider Identifier (RID)	A0 00 00 06 02
Index	F9
Modulus	A5 17 A3 38 85 4E 08 56 EE 4A FD BF 4B DA 5D D3 AB F2 3E 79 FD ED FE 8C E0 87 35 3D 65 C2 F8 90 6A E5 56 98 C7 36 05 EE DC 57 2A 0C 6B 9C E7 26 62 53 DD B4 31 4E 90 51 C8 4E 42 E7 CF 41 7D E4 4C 28 8C 58 4D A7 F5 D2 A8 2E 58 EA 34 3A 7A 23 F4 C2 E5 61 F3 18 E5 A6 50 07 F2 CC 71 13 97 13 F8 62 9E AF A5 ED 19 D5 D9 24 51 EE 0D EB 08 F7 D2 69 74 1C 4D 79 1E 65 48 BE CB C2 49 9D C2 3A 06 29 21 A2 22 56 55 7B 48 71 32 13 B5 AE F7 88 24 C3 7E 78 60 94 C4 AD 3E 0F B5 01 D6 C3 94 B3 A0 44 3E F5 84 52 0F 63 B6 DD AA 82 45 C8 3C 43 F9 58 B8 E9 E0 67 3E 77 98 7E AA 17 E4 CF AD 3B D6 67 D8 88 DA 14 7D 35 C8 33 BB 0B 64 5D 92 15 60 40 61 DD F7 E0 1C 78 04 79 D0 CC AB 07 26 C0 DF 35 AF 11 19 B8 77 3B E9 95 9D C9 7C ED 2A A3 08 87 B4 04 DD DE C1 35 14 6A 6F 24 3E 1D 16 10 6D CA 92 9B 35 61 3C 3D
Exponent	03
Secure Hash Algorithm – 1 Hash	3C 82 2B 8A 2B EC 48 18 1E D0 8E 08 EC 5C 9C 9D 4B 7F 87 92

3. Pencantuman NSICCS CA Public Key di web site ASPI

NSICCS CA Public Key akan tersedia di website ASPI www.aspi-indonesia.or.id