BankAxept
EMV Certificate Authority
Public Keys

Version: 1.33
Last updated: 09.05.2023

TLP:WHITE

Bits AS			
Postaddress: Postboks 2644 0205 OSLO	Visiting address: Hansteensgt 2 OSLO	Phone: +47 23 28 45 10 E-mail: post@bits.no	Org.nr.: NO 971285613

1 Introduction

For EMV offline data authentication, BankAxept provides an EMV CA service which issue Issuer Public Key (IPK) certificates. IPK are used by chip personalizer to issue ICC certificates, which are used during payments for dynamic data authentication (DDA/CDA) and offline PIN encipherment. The terminal service providers use the CA Public Keys to verify that IPK certificates have been issued by the BankAxept CA. The EMV CA for BankAxept is managed Bits AS.

This document contains the Certificate Authority Public Keys for BankAxept and how the keys shall be used in terminals.

1.1 Audience

The audience of this document is primarily terminal service providers.

1.2 Document History

Version	Status	Date	Editor
1.0	First test key published	01.07.2022	E. Bergersen
1.1	Second test key published	16.09.2022	E. Bergersen
1.2	Added UL BTT test key	21.11.2022	S. Bloch
1.31	Added first production key (index 01)	07.12.2022	S. Bloch
1.32	Added that the production public keys only must be used with approved payment solutions supporting offline PIN.	04.01.2023	S. Bloch
1.33	Corrected the year in the date for version 1.32 to 2023. Chapter 5: Added that test keys shall not be used in production terminals.	09.05.2023	S. Bloch

1.3 Change Log

Version	Changes from previous version
1.0	• *Index '81' for test published*
1.1	• *Changed expiry date for index '81'* • *Index '82' for test published*
1.2	• *Added test index 99 for UL BTT test tool*
1.31	• Added production index 01
1.32	• Chapter 2 and 4: Added that the production public keys shall only be used with approved payment solutions supporting offline PIN. • Chapter 2 and 3: Key length changed from 1984 to 1920
1.33	• Corrected the year in the date for version 1.32 to 2023. • Chapter 5: Added that test keys shall not be used in production terminals

1.4 Latest version of the document

Latest version of this document may be obtained on: https://www.bits.no/bankaxept-emv-ca/

1.5 Traffic Light Protocol (TLP)

Bits AS uses TLP in accordance with “FIRST – TLP Standard Definitions and Usage Guidance”. (https://www.first.org/tlp) og (http://www.bits.no/tlp)

As long as copyright is respected, information marked **TLP:WHITE** may be distributed without restrictions.

2 BankAxept Certificate Authority Public Keys

All Certification Authority Public Keys will have December 31 as their planned expiration date. Terminal Service Providers will have a six-month grace period to install new keys, update expiry date and revoke expired keys.

The terminal shall only use BankAxept CA Public Keys distributed by Bits.

The terminal shall have all active BankAxept CA Public keys loaded into the terminals.

The terminal shall only use active BankAxept CA Public keys

The terminal shall remove expired keys within six-months after expiry.

The terminal must be able to store six CA Public keys for BankAxept.

The length of CA Public keys are 1920-bits.

The production BankAxept Public keys shall only be used together with approved payment solutions supporting offline PIN.

3 Format

Field Name	Format	Value Description
key_length	N	Length of CA public key modulus (number of bits) Key length is 1920 bits
expiry_date	AN	YYYY-MM-DD
rid	AN	RID for BankAxept is 'D578000002'
index	N	CA public key index Index '81' to '98' are assigned for test. Index '99' is assigned to UL Brand Test Tool.
hash_algo	N	Identify hash algorithm, '01' is SHA-1
key_algo	N	Identify public key algorithm, '01' is RSA
modulus	H	CA public key modulus
exponent	H	CA public key exponent
key_hash	H	CA public key hash

4 Production Public Keys

The active CA Public keys for BankAxept for production environment is listed below:

Index	Length	Date generated	Active from	Expiry date
01	1920	2022-11-30	2022-11-30	2032-12-31

The production BankAxept Public keys shall only be used together with approved payment solutions supporting offline PIN.

4.1 Index '01'


```
{
   "payment_system":"BankAxept",
   "rid":"D578000002",
   "key_length":"1920",
   "expiry_date":"2032-12-31",
   "index":"01",
   "hash_algo":"01",
   "key_algo":"01",

   "modulus":"C77E3FFF7B98EDA8E7713034A1CC43774199C23E1BFE83B03D4F825741EA68FB97096
   A971D2AD656289DEE3DBE541394CDACB6FFB3A0FFFC2B0209DB54B914B054AFFD38D4088914FF325
   E4E98BEC9D33FBA4B04C90061C513E45FDDB9ACB1576611275F024D6B4EECF07967471CEB911E9C5
   CF16EC0BEDB8F5F3F3127353E7098D534A343C4B3DCF6C1796B2C35589341CAAF79F284D08B44AFD
   FD3D304A2B94A4A26A6B2E5EC497758531C4DF241501EBE494E655B0E58832566BA794124A1249CB
   74C618E296130A3A7439B12A3D1E3757208CA732EF4B4526EB791311D6FEE5AD63FE4A35872DD3DA
   E5A51A3802D",
   "exponent":"03",
   "key_hash":"6D38D80729B03C7AD8C1F3609E481675B76BB278"
}
```

5 Test Public Keys

The active CA Public keys for BankAxept for test environment is listed below:

Index	Length	Date generated	Active from	Expiry date
81	1984	2022-06-13	2022-07-01	2022-12-31
82	1920	2022-09-07	2022-09-07	2032-12-31
99 (UL BTT test tool)	1408	2022-11-18	2022-11-18	2028-12-31

Test keys shall not be used in production terminals.

5.1 Index '81'


```
{
   "payment_system":"BankAxept",
   "rid":"D578000002",
   "key_length":"1984",
   "expiry_date":"2022-12-31",
   "index":"81",
   "hash_algo":"01",
   "key_algo":"01",
   "modulus":"A94B15E5D7A5A9DF1A81F96C564AA0FDD2F2665213E1DA433EC8AB0DA363BC524E4DA
   F552BF29A66C062693DB855870D4D88C1E44A83B1ADD6079A7223CD24920E9382424E9F5577B5D3D
   C7B40D4273589CC4337346310A6A6917150E5A626F7066368410354361AC121491A1CE15F38955E4
   40E2F56884DB3DE29622291EF147A1A0ED27B2F051584E8ED95EBBF3B02070E1A506BBCA5A6ED198
   CFC090956AAF11D4215E41BC8596AF010A03EF559CABD55D77F19770505C4B027DD5926E5ECB3829
   3DD227D8937CADBC4F790FAF0D8E41CA217DAC44307CCC17ECA8A6BA3F4EE513AA12E39A1DC1EB5E
   BFA1806C4A4368B786F77026723",
   "exponent":"03",
   "key_hash":"E643B97A0877E328FD16AB868564D80CC6BB9867"
}
```


5.2 Index '82'


```
{
   "payment_system":"BankAxept",
   "rid":"D578000002",
   "key_length":"1920",
   "expiry_date":"2032-12-31",
   "index":"82",
   "hash_algo":"01",
   "key_algo":"01",
   "modulus":"EE7758C22711958D6E0FA05362CB9598EB0073AF49CAE8B37DEC39B1E179194195B4E
   26BDA6EEAD8D981389FD9B3E75FD69DFF07F79617C957979A337F0A77122CA573F5577E63A20ED47
   95FABD9F337479E7BAE5D1A367E23F2F820A2C6F4FD07EBEA87A08F6CA39B48A1CAC1D28A5C68C8B
   C584834869EF061FA27C260B64EAD8BB7A104D8787004F6013AE7B9143FD6874C3BA3974F3122A3B
   EAD8D333F702CC0D3DD0F9CE5AD59BBDB5E88C995C3D1AEFD025E057C73BAD4347C5BD925AB32D3D
   A1FBAC83790D5BE5A47DF2AC17D0D9A278DA8F2B95EAFE1131B23DFD9457C84F1DD8E1A19DA6AB9E
   7C3DB08E04D",
   "exponent":"03",
   "key_hash":"A0262E62AD39C5C6BF70A15F46F9CD51DF176E1D"
}
```

5.3 Index ‘99’


```
{
   "payment_system":"BankAxept",
   "rid":"D578000002",
   "key_length":"1408",
   "expiry_date":"2028-12-31”
   "index":"99",
   "hash_algo":"01",
   "key_algo":"01",
   "modulus":"87B26154BA85F4247CCD54A795885A01FF3724D0C642158FFC843B9F3C2E8F0775725
   3A6DECBA6A36EF991626D83D1078DB2B5446A27C580EE94133E84D220690E681654E2BEDF147A5FB
   362C23E8764C04AA1335F9BE23F83E34102D716B2989EBEFFD8BA7751E451DBC6CE19D305E65ACF0
   88BACBE7F9DA0480A2897D24AF97F0D44B8796621381DECD648C8216448A5FB5D8A366132FCE192D
   046F4156D2CA88301A7087725D7FE87492588CAC38D",
   "exponent":"03",
   "key_hash":"1501F3EBC172F6609AE817521BB448EA25911447"
}
```