



BankAxept EMV Certificate Authority Public Keys

Version: 1.1
Last updated: 16.09.2022

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

1.3 Change Log

Version	Changes from previous version
1.0	<ul style="list-style-type: none">• Index '81' for test published
1.1	<ul style="list-style-type: none">• Changed expiry date for index '81'• Index '82' for test published

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 1984-bits.

3 Format

Field Name	Format	Value Description
key_length	N	Length of CA public key modulus (number of bits) Key length is 1984 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

4.1 Index 1

Not generated yet.

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

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"
}
```