MyEID PKI Smart Card

Authenticity Verification

Table of contents

Version	Author	Date	Comment
1	HH	2026-03-16	Initial version

1 Introduction

Aventra's MyEID PKI Smart Card contains a mechanism to verify authenticity of the card cryptographically. The purpose of the mechanism is to provide proof that a MyEID card is the authentic, certified version, which security features have been verified to be secure by evaluators.

The mechanism is based on public key cryptography. Aventra publishes public keys, and the corresponding private keys are only in possession of and stored securely by Aventra. Authentication data, which comprises a public key of unique, card-specific key pair, is signed using the private key in Aventra's production. Validity of the signature can be verified using the public keys published by Aventra.

Aventra may create new key pairs for this purpose any time. This document contains information about which public keys should be used to verify a specific MyEID version produced at specified time. The verification mechanism is described in MyEID PKI Smart Card Reference Manual, which is available for download at https://aventra.fi

2 Public keys

The following public keys are valid for verifying Common Criteria EAL4+ certified MyEID version 5.0.0 produced since 2025 until further notice.

MyEID Factory Root	04 55 4c 22 cf d4 6b e3 5f d4 1e 35 0f e2 7b d6 67 ad c3 45 9b 81 dd 84 2e 4f 3d 74 51 a1 af 6b e2 ef 69 de 30 34 1e 70 5d 2b ee d1 df 0a f6 ab 22 99 68 70 ce 63 c7 45 4a 56 04 66 45 9e 53 3c ba 29 fa 88 32 3e 7f c7 a1 fd c3 a9 73 57 0a aa c8 85 01 f7 9c 35 1d 3f 2f d4 f2 0f a6 a7 b8 f2 3b
MyEID 5.0.0 CC Card Signing Key	04 85 d0 ad 9d 5b 54 f9 61 ae 6c dc 7c 44 16 fd 98 e2 0d 6e 96 e3 bf 27 d2 62 a6 61 74 66 ea c6 dc fc 19 41 9a be aa b9 8e d4 c2 b4 0c 2b a1 d5 85 bd 52 36 93 bc b3 85 8c b5 a7 8b f6 3b f5 a6 ba 4d e1 58 39 6b b5 3a 9d 1c 22 4c b9 07 b5 bd d9 09 f6 5b 84 66 ca dc fc f0 df 9e 70 03 a5 ec a0

3 Certificates

The public keys are also delivered in X.509 certificates. The certificates are available for download at Aventra's web site at http://aventra.fi

Subject common name	**Thumbprint**
MyEID Factory Root	08e67e6d8db3ed37dd079c3010232e6e653d5f78
MyEID 5.0.0 CC Card Signer	e3a394004cffda2f40dcfb9255bbd38291072be0