Dument title:

SealSQ Trusted Platform Module (TPM) Endorsement Key (EK) Certificate Chain

HISTORY

Version	Date	Author	Comments
1.0	December 15, 2025	Jerome DI MARTINO	First release
1.1	January 20, 2026	Jerome DI MARTINO	Update SEALSQ TPM 384p Intermediate CA
1.2	February 17, 2026	Jerome DI MARTINO	Update CA certs and add CRL

TABLE OF CONTENTS

1 GENERAL

1.1 Introduction

The Endorsement Key Certificate Chain (EK Certificate Chain) is a foundational element of hardware-based identity. It ensures that a TPM (Trusted Platform Module) originates from a legitimate manufacturing process, that it owns a unique and tamper-proof identity, and that it can be integrated with confidence into secure ecosystems and provisioning workflows. This document describes the structure, purpose, and implementation of the EK Certificate Chain used in our company.

1.2 References

This document is intended for the product team comprising:

- TPM 2.0 TCG doc v1.83 https://trustedcomputinggroup.org/resource/tpm-library-specification/

2 STRUCTURE OF THE EK CERTIFICATE CHAIN

The EK chain consists of multiple hierarchical trust levels. In our PKI architecture, it typically includes:

1. **Root CA (Endorsement Root CA)** — Offline internal root authority.
2. **Subordinate CA (Endorsement Sub CA)** — Subordinate CA dedicated to EK signing.
3. **EK Certificate** — Device-specific certificate.

3 SEALSQ TPM HIERARCHY FOR EK CERTIFICATES

3.1 SealSQ TPM Root Certification Authorities

TPM Root CA RSA4096 G1

Subject name	Common Name: TPM Root CA RSA4096 G1, Organization: SealSQ, Country: CH
Issuer name	**Common Name: TPM Root CA RSA4096 G1, Organization: SealSQ, Country: CH**
Name Hash	**1BED9DC07B2CDC4DCE9AEF3C8757D894F3E52A68**
Subject Key Identifier	**D33F1FD0D457E33A365F30C71A478779D2748EB6**
Authority Key Identifier	**D33F1FD0D457E33A365F30C71A478779D2748EB6**
Thumbprint	**F3C3619E9282FCE25EC430F751D7F4608F3CC8A2**
CA cert	http://public.wisekey.com/crt/tpmrca4096g1.crt http://public.wisekey.com/crt/tpmrca4096g1.cer
CA CRL	http://public.wisekey.com/crt/tpmrca4096g1.crl

TPM Root CA 256p G1

Subject name	Common Name: TPM Root CA 256p G1, Organization: SealSQ, Country: CH
Issuer name	**Common Name: TPM Root CA 256p G1, Organization: SealSQ, Country: CH**
Name Hash	**383CA32BFF366299527380E24AC8C0F76BA936CF**
Subject Key Identifier	**72C7DCEC3F9A2A5B1AF3D6CA10CE50C654DA068D**
Authority Key Identifier	**72C7DCEC3F9A2A5B1AF3D6CA10CE50C654DA068D**
Thumbprint	**9C1CF5B34024B404D0645B3847B547712336B089**
CA cert	http://public.wisekey.com/crt/tpmrca256pg1.crt http://public.wisekey.com/crt/tpmrca256pg1.cer
CA CRL	http://public.wisekey.com/crt/tpmrca256pg1.crl

TPM Root CA 384p G1

Subject name	Common Name: TPM Root CA 384p G1, Organization: SealSQ, Country: CH
Issuer name	**Common Name: TPM Root CA 384p G1, Organization: SealSQ, Country: CH**
Name Hash	**5447BDA6C12CE2B09E4CE983AD28510552A41D52**
Subject Key Identifier	**FF1D382E7BB340A9BB477789FD72C63916F4739D**
Authority Key Identifier	**FF1D382E7BB340A9BB477789FD72C63916F4739D**
Thumbprint	**9BC8BB46718FAFA7B9128A77A5F08FFF6A824BBD**
CA cert	http://public.wisekey.com/crt/tpmrca384pg1.crt http://public.wisekey.com/crt/tpmrca384pg1.cer
CA CRL	http://public.wisekey.com/crt/tpmrca384pg1.crl

3.2 SealSQ TPM Subordinate Certification Authorities

SEALSQ TPM RSA4096 Intermediate CA

Subject name	Common Name: SEALSQ TPM RSA4096 Intermediate CA, Organization: SealSQ, Country: CH
Issuer name	**Common Name: TPM Root CA RSA4096 G1, Organization: SealSQ, Country: CH**
Name Hash	**58A45456B28A430E907F5390F8CF2754FA2F3AC2**
Subject Key Identifier	**24529642C119641B766243B8876474E87FC44A86**
Authority Key Identifier	**D33F1FD0D457E33A365F30C71A478779D2748EB6**
Thumbprint	**EBE4E4CBCF402FEB21AC005359858BE878656DB1**
CA cert	http://public.wisekey.com/crt/tpmica4096tpm001.crt http://public.wisekey.com/crt/tpmica4096tpm001.cer
CA CRL	http://public.wisekey.com/crt/tpmica4096tpm001.crl

SEALSQ TPM 256p Intermediate CA

Subject name	Common Name: SEALSQ TPM 256p Intermediate CA, Organization: SealSQ, Country: CH
Issuer name	**Common Name: TPM Root CA 256p G1, Organization: SealSQ, Country: CH**
Name Hash	**4DC20F23C4EF6233703B9E4BE4FEF131B00D10AA**
Subject Key Identifier	**0B3C824339FB637AD9EA8F376856EFE6E572C618**
Authority Key Identifier	**72C7DCEC3F9A2A5B1AF3D6CA10CE50C654DA068D**
Thumbprint	**031B934D49028D9DFB0944372299E1F66B9579EC**
CA cert	http://public.wisekey.com/crt/tpmica256ptpm001.crt http://public.wisekey.com/crt/tpmica256ptpm001.cer
CA CRL	http://public.wisekey.com/crt/tpmica256ptpm001.crl

SEALSQ TPM 384p Intermediate CA

Subject name	Common Name: SEALSQ TPM 384p Intermediate CA, Organization: SealSQ, Country: CH
Issuer name	**Common Name: TPM Root CA 384p G1, Organization: SealSQ, Country: CH**
Name Hash	**6A9D4B218E0BE8ABA40A54FFA512B4F7E2BC005C**
Subject Key Identifier	**15505F6A59F48A03DCA19B8C3226FEAC1B921EBA**
Authority Key Identifier	**FF1D382E7BB340A9BB477789FD72C63916F4739D**
Thumbprint	**CA07D4FFF9C24C5BC12357E2039AEC009D008365**
CA cert	http://public.wisekey.com/crt/tpmica384ptpm001.crt http://public.wisekey.com/crt/tpmica384ptpm001.cer
CA CRL	http://public.wisekey.com/crt/tpmica384ptpm001.crl

4 REQUIRED STEPS FOR READING AND VERIFYING THE EK CERTIFICATE FROM SEALSQ TPM

A customer may validate a TPM by:

1. Verifying the EK → Sub CA → Root CA certificate chain.
2. Checking internal OIDs (policies, manufacturing identifiers).
3. Confirming that the EK corresponds to the TPM via attestation commands.
4. Performing a cryptographic challenge using the EK or a derived AIK.