

---

# Certification Practice Statement

---

SekChek IPS

---

May, 2010

---

---

First Published: April, 2008  
Last Revision (3): May, 2010

Copyright © 2008-2010, SekChek IPS  
Tel: +27 (11) 461 7900  
[inbox@sekchek.com](mailto:inbox@sekchek.com)  
[www.sekchek.com](http://www.sekchek.com)

## Contents

---

1.	Purpose of this Document	3
2.	SekChek IPS	3
3.	SekChek Software	3
4.	SekCert Digital Certificate	3
5.	SekChek's PKI Hierarchy	4
6.	Certificate Identifiers	4
7.	Key Lengths & Certificate Expiry Dates	4
8.	Security of SekCert's Private Key	5
9.	Certificate Revocation	5
10.	Authority Information Access	6
11.	Physical Access & Environmental Controls	6

# SekChek: Certification Practice Statement

---

## 1. Purpose of this Document

This document defines SekChek's Certification Practice Statement (CPS) including the various technical standards and practices employed for approving, issuing and managing the SekCert digital certificate.

This is a public document, which is available on request from SekChek.

## 2. SekChek IPS

SekChek IPS provides an automated computer security review and security benchmarking service, which compares security controls against international leading practices and real-world industry averages for security.

The service may require a data file to be transferred to SekChek's premises for processing and analysis.

## 3. SekChek Software

The SekChek software includes utilities for encrypting data files as well as digital certificates to support the use of public key encryption techniques. The required certificates are installed and registered by default and when the client selects SekChek's public key encryption option (Options | Use Public Key Encryption).

The SekChek software encrypts a client's data file using several layers of encryption, including an outer layer that employs public key encryption techniques. The public key encryption layer uses a certificate named SekCert, a component of the SekChek software.

## 4. SekCert Digital Certificate

The SekChek software uses the public key defined in the SekCert certificate, together with the Rivest, Shamir, Adelman (RSA) and Triple Data Encryption Standard (3DES) encryption algorithms, to asymmetrically encrypt a client's data file.

Because the SekCert certificate's public key is cryptographically bound to a matching private key, a data file encrypted with the certificate can only be decrypted with the associated private key. This private key resides at SekChek's secure premises.

The content of the SekCert certificate includes, but is not limited to:

- Serial Number of the digital certificate
- Algorithm types
- Issuing certification authority (SekChekSubOrdinateClients)
- Validity period of the digital certificate
- Name / Subject of the certificate (SekCert)
- Certificate's public key
- Length of the public key
- Thumbprint of the certificate
- Hash algorithm used to generate the thumbprint

# SekChek: Certification Practice Statement

## 5. SekChek's PKI Hierarchy

SekChek employs a 3-tier Public Key Infrastructure (PKI) consisting of a Root CA, Intermediate / Issuing CA and the SekCert certificate itself. The SekCert certificate is issued by the SekChekSubOrdinateClients CA.

The following table defines SekChek's policy for certificate validity periods and maximum renewal periods. SekChek's policy is to renew the private / public key pair at the 'Renew After' interval.

Certificate Name	Function	Validity Period	Renew After
SekChekRootCA	Root CA	25 years	10 years
SekChekSubOrdinateClients	Intermediate / Certificate Issuing CA	10 years	5 years
SekCert	Encryption Certificate	3 years	2 years

## 6. Certificate Identifiers

The following table identifies the current certificates used by SekChek. All thumbprints were created with Secure Hash Algorithm 1 (sha1).

Certificate Name	Serial Number	Thumb Print
SekChekRootCA	5a ce ea 14 22 50 d7 a0 45 a5 94 fd 49 87 a5 c7	18 06 84 9e 78 6d e1 a2 5f 26 aa 16 bc 0c 9b 7a b4 b6 8f 98
SekChekSubOrdinateClients	17 29 36 3f 00 00 00 00 00 05	96 1b b1 58 e8 10 71 77 6a 6e d7 3f 79 16 00 44 cb 69 e4 6d
SekCert	36 aa 93 ca 00 01 00 00 00 cb	b3 dc 75 e1 12 68 58 aa 34 80 58 af 91 59 06 44 06 2f c4 ff

## 7. Key Lengths & Certificate Expiry Dates

SekChek uses a key length of 4096 bits for all certificates, including the SekCert certificate.

The key pair for the SekChekSubOrdinateClients CA was last renewed in April 2006. The fifth version of the SekCert certificate was issued in April 2010.

Certificate Name	Key Length	Issue Date	Expiry Date
SekChekRootCA	4096 Bits (RSA)	1 September 2003	1 September 2028
SekChekSubOrdinateClients	4096 Bits (RSA)	21 April 2006	21 April 2016
SekCert	4096 Bits (RSA)	07 April 2010	06 April 2013

# SekChek: Certification Practice Statement

## 8. Security of SekCert's Private Key

The private key for the SekCert certificate resides on a secure Server located inside SekChek's domain.

The private key is marked as 'non-exportable' on the Server. Access to the service that uses the private key to decrypt data files is controlled via a special user account, which is only used to start the service. The password for the account is restricted to trusted Operations personnel who are responsible for starting the service.

SekChek employs the following security standards to secure access to the special user account that provides access to the SekCert certificate's private key.

- Minimum Password Length: 8 characters
- Password Stored in Non-Reversible Encrypted Format: Yes
- Password Complexity Controls: Yes
- Password Change Frequency: 35 days
- Controls to Prevent Password Cycling: Yes
- Intruder Detection Controls: Maximum 3 password guessing attempts in a 24 hour period, indefinite lockout of the account
- Audit Trail of Usage: Yes
- Private Key Exportable: No

The private key for SekChek's root CA is stored offline on physically secured media in encrypted format. Access to the storage media containing the private key is restricted to the organisation's CEO.

Changes to the SekCert certificate, including the renewal of key pairs are authorised and managed by the CEO.

## 9. Certificate Revocation

The purpose of certificate revocation is to permanently end the operational life of a certificate before its natural expiry date is reached.

SekChek will revoke a certificate in the event of loss, theft, modification, unauthorised disclosure, or any other compromise of the certificate's private key.

The Certificate Revocation List (CRL) for the SekChekSubOrdinateClients CA is typically published on SekChek's web site every 14 days. However, under certain circumstances, the CRL may be published more frequently.

The following table lists the CRL Distribution Points (CDPs) for the SekChekSubOrdinateClients and SekCert certificates.

Certificate Name	Certificate Revocation List (CRL)
SekChekRootCA	-
SekChekSubOrdinateClients	<a href="http://www.sekchek.com/certsrv/certenroll/SekChekRootCA.crl">http://www.sekchek.com/certsrv/certenroll/SekChekRootCA.crl</a>
SekCert	<a href="http://www.sekchek.com/certsrv/certenroll/SekChekSubOrdinateClients.crl">http://www.sekchek.com/certsrv/certenroll/SekChekSubOrdinateClients.crl</a>

# SekChek: Certification Practice Statement

---

## 10. Authority Information Access

The following table lists the paths to the certificates / public keys for the SekChekRootCA and SekChekSubOrdinateClients CAs. The certificates are also embedded in the SekChek software.

Certificate Name	Authority Information Access (AIA)
SekChekRootCA	<a href="http://www.sekchek.com/certsrv/certenroll/SekChekRootCA.crt">http://www.sekchek.com/certsrv/certenroll/SekChekRootCA.crt</a>
SekChekSubOrdinateClients	<a href="http://www.sekchek.com/certsrv/certenroll/SekChekSubOrdinateClients(1).crt">http://www.sekchek.com/certsrv/certenroll/SekChekSubOrdinateClients(1).crt</a>

## 11. Physical Access & Environmental Controls

Access to the Server that contains the private key for the SekCert certificate is controlled by several layers of security:

- SekChek's premises are located inside a secure, restricted complex with access booms controlled via a swipe card system
- All entry points to the complex are manned by security personnel
- The perimeter of the complex is monitored on a 365 x 24 hour basis by cameras and patrolled by security guards
- SekChek's premises are alarmed and protected by a 24-hour armed response company
- SekChek's premises do not have any signage; we do not publish our physical address
- Access to SekChek's premises and computer rooms is controlled by a card access system that records all inbound and outbound access
- Entry to computer rooms is controlled via a swipe card system that restricts access to essential Operations personnel.
- Servers are secured to the floor or housed inside locked cages to restrict physical access to the hardware
- Temperature and humidity inside Server rooms are controlled by appropriate air conditioner units
- SekChek has taken reasonable precautions to ensure its premises are adequately protected against damage by fire and flooding
- SekChek's Servers are supported by primary and secondary power systems, which ensure continuous, uninterrupted access to electric power