Australian Government
Security Construction and Equipment Committee

Class C Keying Systems Policy

Handling instructions

This document is protectively marked OFFICIAL: Sensitive, which means it contains information which if compromised may cause limited damage to national security, Australian Government agencies, commercial entities or members of the public.

You must take all reasonable action to protect and maintain the security of this document. This information should be shared only with individuals within your agency with a demonstrated 'need-to-know'.
This document must be stored in a lockable container and shredded before disposal. This document may be stored on electronic media but access must be limited to individuals within your agency with a demonstrated 'need-to-know'. Portable electronic media containing this document must be stored, handled and disposed of in accordance with the Australian Government *Protective Security Policy Framework* and *Information security manual*.

Disclaimer

The Commonwealth, its officers, employees, and agents exclude all liability for loss or damage (including in negligence) suffered or incurred by any organisation or individual as a result of their use of or reliance upon the information contained in this document.

FOI statement

This document and any information, extract or summary from this document, is exempt under the Freedom of Information Act 1982. Refer related FOI requests to the Attorney-General's Department, Canberra.

Inquiries

Inquiries should be addressed to:

Chair of the Security Construction and Equipment Committee (SCEC)

GPO Box 1508

Canberra, ACT, 2601

Ph: 02 6234 1217

Email: scec@scec.gov.au

Release history

Version No.	Issue Date	Nature of Amendment
1.00	07-DEC-2009	Draft final for presentation to SCEC
1.01	22-FEB-2010	Final
2.00	09-AUG-2019	Policy review - Approved by SCEC on 09 August 2019

Contents

1 Introduction

Class C keying systems are approved by the Security Construction Equipment Committee (SCEC) for exclusive use in Australian Government Class C applications; such as Class C containers, Type 1A Security Alarm System panels, and other Class C applications as approved by the Chair of SCEC.

This document sets out the policy requirements for the production and ongoing management of Class C keying systems.

1.1 Reference Documents

Document Number	Version	Document Title
A2037339	5	TC-020 Keying Systems (Test Criteria)
A15986685	1	TC-032 Class C Keying Systems (Test Criteria)
A16695583	1	PAC-028 Class C keying systems (Pre Acceptance Criteria)
A16694767	1	Application form - Class C Keying Systems

2 Definitions

2.1 Abbreviations

Abbreviation	Definition
T4	T4 is the Protective Security area within ASIO

2.2 Acronyms

Acronym	Definition
ASIO	Australian Security Intelligence Organisation
PAC	Pre-Acceptance Criteria
SCEC	Security Construction Equipment Committee
SEEPL	Security Equipment Evaluated Products List
TC	Test Criteria

2.3 Terms

2.3.1 Class C

A Class C keying system is a keying system for use exclusively on Class C containers, and selective other applications including securing Type 1A Security Alarm System panels, and IT server racks housing sensitive IT infrastructure.

A Class C keying system must meet all the requirements for an SL3 keying system, with some additional requirements relating to the management of these systems.

2.3.2 Manufacturer / Original Equipment Manufacturer (OEM)

A manufacturer is considered the original owner/designer of a keying system technology. Usually, manufacturers do not sell keying systems directly to the public. Rather they will sell their product to approved dealers or agents. Manufacturers routinely use contractual agreements with their dealers or agents to ensure their keying systems are managed with the appropriate level of security.

2.3.3 SCEC-approved locksmith

A SCEC-approved locksmith is a professional locksmith that has undergone training in the unique requirements of working in a national security classified facility. SCEC-approved locksmiths, when listed on the live SCEC-approved locksmiths list found on the SCEC website, are permitted to work on Class C applications.

2.3.4 Entity

An entity may be a SCEC-approved locksmith, Government department, company, or an individual that has been approved in writing by the Chair of SCEC (or their representative) to order Class C keying systems and components from the OEM.

2.3.5 SCEC-approved locksmiths list

The SCEC-approved locksmiths list is a live list of all currently approved locksmiths. This list is available on the SCEC website. Any locksmith that does not appear on the live list (even if in possession of a SCEC-approved ID card) is not approved by SCEC to handle Class C products or information.

2.3.6 Class C products

For the purposes of this document, the term ‘Class C Product’ refers to Class C keying system products only, i.e. a Class C cam lock or Class C oval cylinder.

2 Requirements

Class C keying systems, OEMs, and entities, must meet various requirements and standards, including technical, procedural, and administrative, as set out in this document.

Any request for a deviation of the requirements set out in this document must be made, in writing, to the Chair of SCEC.

Requests for approval to deviate from this policy will only be accepted from OEM's, or the Agency Security Advisor (ASA) or Chief Security Officer (CSO) of the end user (Australian Government department).

SCEC can be contacted via:

Phone	Website	Email	Post
+61 2 6234 1217	www.scec.gov.au	scec@scec.gov.au	Chair of SCEC GPO Box 1508 Canberra, ACT, 2601

3 Keying system

The keying system requirements are:

- Must meet the requirements of a SCEC-approved keying system at SL3 or SL4 (Test Criteria TC-020 Keying Systems - A2037339);
- Must have a unique profile, used exclusively in Class C applications;
- The OEM will produce only one Class C profile per keying system;
- The phrase 'Class C', or any reference to the Australian Government, must not be marked on the key or cylinder;
- The key code must be indirect, that is, the key bitting must not be obtainable from the key code;
- The key code must be marked on a disposable tag provided with the keys;
- The key code must not be marked on the key or cylinder;
- Two keys will be provided with each cylinder;
- Cylinders must not be keyed alike (except for conditions set out in section 7.1); and,
- Cylinders must not be master keyed or use master discs/pins/coding components for assembly.

4 Class C products

4.1 Applications

Class C keying systems may only be installed on:

- SCEC-approved Class C Containers;
- An after-hours lock on Class C rooms;
- Type 1A enclosures;
- SCEC-approved electronic key cabinets; or,
- Any other application where written approval from the Chair of SCEC (or their representative) has been provided.

4.2 Oval cylinder

- Must have written approval from the Chair of SCEC (or their representative) for each cylinder ordered.
- Must have a unique part number.
- Must suit Australian mortice locks, as per the dimensions set out in Figure 1.

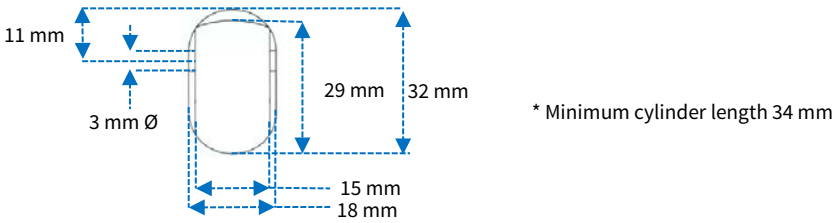

Figure 1: Oval cylinder dimensions

4.3 Cam locks

- May have one or two key removal positions.
- Must have a unique part number.
- Must meet the dimensions shown in Figure 2.
- Cams are provided by the container manufacturer. The cam lock must secure cams using a locking nut, and not a screw, as shown in Figure 2.
- Must also include a mechanism, such as a shaker washer, to prevent the locking nut from coming loose over time.

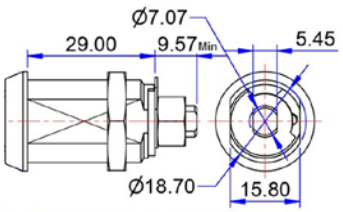

Figure 2: Cam lock dimensions

4.4 Other cylinder types

The OEM must request authority from the Chair of SCEC, in writing, before producing any other type of cylinder or locking device, other than those set out in sections 4.1 and 4.3, on a Class C profile.

5 Supply/Sale of Class C keying systems

- Cylinders and keys may only be supplied to an entity on the live SCEC-approved locksmith list, or to an entity where written authorization has been provided to the OEM by the Chair of SCEC (or their representative).
- Class C profiles must not be used for any application other than Australian Government Class C environments.
- Class C products must be signed for by the entity on delivery.

6 Handling and storage of components and information

- The OEM must manage, in house, all manufacture of components unique to the Class C profile. That is, the OEM must not outsource the manufacture of components that are unique to the Class C profile (i.e. barrels and keyblanks), without written approval from the Chair of SCEC (or their representative).
    - Where written approval is provided by the Chair of SCEC (or their representative), all documentation and correspondence between the OEM and the outsourced supplier(s) must not make any reference to Class C (including part numbers), the Australian Government, ASIO, T4 Protective Security, or SCEC.
- Key codes must not be attributable to an entity or Government Department after sale/dispatch.
- Access to components and Class C information (including entities and coding data) is limited to Australian citizens only.
- Sensitive information about the Class C system, such as key codes and entity order history, must be generated and stored only via IT systems where the 'essential eight' strategies to mitigate cyber security incidents have been applied. The strategies to mitigate cyber security incidents are published by the Australian Cyber Security Centre (ACSC); further information can be found via the Australian Signals Directorate (ASD) website.

7 Cylinder coding

- The OEM must manage, in house, all coding and assembly for Class C products. That is, the OEM must not allow any of these activities to be undertaken by any other party, including SCEC-approved locksmiths.
- Cylinder coding must be determined via an unpredictable and random coding process.
- Key code numbers must be random, that is, the key combination must not be derivable from the code number.
- Two keys must be provided with each cylinder.
- The terms 'Australian Government' or 'Class C' must not appear on either the cylinder or the key.
- The key code number must not appear on the cylinder or the key.
- The key code must be provided with the keys on a detachable key tag. This tag must show only the key code number only, and no other information.
- All cylinders must be assembled to different coding (keyed to differ), unless the conditions set out in section 7.1 are met.

7.1 Multiple cylinders on the same code

The OEM may provide cylinders to an entity on the same code (keyed alike), only in the situations detailed below:

- Two cam locks may be provided keyed alike when the entity confirms to the OEM, in writing, that they are for installation into a server rack, and both of the cam locks will be installed on the same rack and accessing the same space (i.e. two doors on the same server rack). In this instance, only two keys in total will be issued with the pair of cam locks;
- Multiple cam locks may be provided keyed alike when the entity confirms to the OEM, in writing, that they are for installation into an electronic key cabinet for the purposes of retaining a stored key to hide that key's bitting. In this instance, only two keys in total will be issued for all of the cam locks;
- Multiple oval cylinders may be provided keyed alike when the entity confirms to the OEM, in writing, that they are for installation into doors securing a Class C room, where both doors provide access to the same space. In this instance, only two keys in total will be issued for all of the cylinders;
- Multiple cam locks may be provided keyed alike when the entity confirms to the OEM, in writing, that they are for installation into multiple cabinets housing Type 1A Security Alarm System (SAS) components, and each cabinet contains only components for the same Type 1A SAS. In this instance, only two keys in total will be issued for all of the cam locks; or,
- The chair of SCEC (or their representative) has approved, in writing, the sale of more than one cylinder on the same code.

8 Key cutting

- The OEM must manage, in house, all key cutting for Class C systems. That is, the OEM must not allow any Class C keys to be cut by any other party, including SCEC-approved locksmiths.
- Only two keys may be cut for a Class C cylinder (unless the conditions set out in section 8.1 are met).

8.1 Additional keys

Additional keys may only be cut where one of the two conditions below are met:

a) The new key is replacing a damaged key. In this situation:
   - Before the new key is cut at least 90% of the damaged keys' bitting must be returned to the OEM;
   - The OEM must destroy the remnants of the damaged key to an extent that a qualified locksmith could no longer determine the key bitting;
   - Only one replacement key may be cut per damaged key; and,
   - The OEM must document the date and conditions of the destruction of the 90% of the damaged key

b) The chair of SCEC has approved, in writing, the cutting of additional key(s)

9 Requirements of the OEM:

The OEM must adhere to the below requirements

- The OEM must manage all manufacture of components, coding, assembly, and key cutting for Class C products;
- The OEM must not provide raw Class-C components (Class C barrels or key blanks) to any party;
- Cylinders and keys must only be supplied to an entity on the SCEC-approved locksmith list, or where the OEM has received written authorization from the Chair of SCEC (or their representative) to supply Class C products to that entity;
- OEMs must reference the live SCEC-approved locksmith list on the SCEC website for every Class C order;
- Class C profiles must not be used for any application other than Australian Government Class C environments;
- Key codes must be determined via an unpredictable coding process;
- Key code numbers must be random, that is, the key combination must not be derivable from the code number;
- Access to components and Class C information (including entities and coding data) is limited to Australian citizens only;
- Key codes must not be attributable to an entity or Government Department after sale/dispatch; and,
- Sensitive information about the Class C system, such as key codes and entity order history, must be generated and stored only via IT systems where the 'essential eight' strategies to mitigate cyber security incidents have been applied. The strategies to mitigate cyber security incidents are published by the Australian Cyber Security Centre (ACSC); further information can be found via the Australian Signals Directorate (ASD) website.

10 Requirements of the SCEC-approved locksmith:

The SCEC-approved locksmith must adhere to the below requirements

- The SCEC-approved locksmith must ensure that their SCEC approval remains current, and that their details are accurately reflected on the SCEC-approved locksmiths list on the SCEC website;
- Class C key bitting must not be recorded;
- Class C key codes must not be recorded;
- Class C products must only be installed in Class C applications;
- Class C cylinders must not be re-coded (rekeyed) for any reason;
- Class C cylinders are for replacement only, and must not be on sold or used in new installations; and,
- Any request for a Class C product, or for work to be undertaken on a Class C product, that is in contravention of this policy must be referred to the Chair of SCEC. Approval must be received from the Chair of SCEC (or their representative), in writing, before the work may be undertaken.

11 Requirements of the end user (Government department):

The end user (Government Department) must adhere to the below requirements:

- Where a Class C key cannot be located, the Class C cylinder must be replaced as soon as practicable (including any other cylinders that may operate on the same key).

12 Audit process

The OEM, SCEC-approved locksmiths, and any entity that has been authorized by SCEC to receive Class C products, may be subject to audit by ASIO-T4; the timing and content of the audit is at the discretion of ASIO-T4. ASIO-T4 may request information relating to the Class C process, such as:

- Records of orders for any Class C product. This may include information relating to the entity making the order, the content of the order, delivery methods of orders, etc.
- Records of special requests including documentation as for standard orders, plus evidence that appropriate approvals were obtained from the Chair of SCEC (or their representative).
- Copies of the OEM or entities internal policies detailing how Class C products are handled, such as:
    - Process for storage and handling of Class C components and information
    - Restriction of access to coding and entity information to staff with a need to know
- Evidence of the OEM, SCEC-approved locksmith, or entities IT infrastructure, detailing how it meets the requirements set out in this policy. i.e. the 'essential eight' strategies to mitigate cyber security incidents have been applied. The strategies to mitigate cyber security incidents are published by the Australian Cyber Security Centre (ACSC); further information can be found via the Australian Signals Directorate (ASD) website.