



CCOW Application Protection Package (CCOWAPP)

April 2008

Version 1.1

Editor:

David Staggs
Veterans Health Administration (SAIC)

Copyright © 2008 Health Level Seven International ® ALL RIGHTS RESERVED. The reproduction of this material in any form is strictly forbidden without the written permission of the publisher. HL7 International and Health Level Seven are registered trademarks of Health Level Seven International. Reg. U.S. Pat & TM Off.

IMPORTANT NOTES:

A. If you are the individual that downloaded or ordered this HL7 Standard, specification or other work (in each and every instance "Material"), the following describes the permitted uses of the Material.

B. If you are NOT such individual, you are not authorized to make any use of the Material. To obtain an authorized copy of this Material, please visit <http://www.hl7.org/implement/standards/index.cfm>.

C. If you are not an HL7 Organizational Member, the following are your permitted uses of this Material:

- 1. Read and Copy License Only.** HL7 hereby grants you the right, without charge, to download and copy (for personal use only) this Material for study purposes only. This license grant does not include the right to sublicense or modify the Material, or to implement the Material, either in whole in part, in any product or service.

Please see <http://www.hl7.org/legal/ippolicy.cfm> for the full license terms governing the Material.

D. If you are an HL7 Organizational Member, the following are your permitted uses of this Material.

1. Implementation License Terms.

1.1 Definitions. As used in this Agreement, the following terms shall have the following definitions:

"Compliant Product" is a product or service that implements Material that is an HL7 Specification in whole or in part.

"End User" is a company, entity or individual that is the ultimate purchaser or licensee from Licensee of a Compliant Product.

1.2 License. In consideration of becoming an Organizational member of HL7 and continuing to pay the appropriate HL7 Organizational membership fees in full, HL7 hereby grants to you without additional charge, on a perpetual (except as provided for in the full license terms governing the Material), non-exclusive and worldwide basis, the right to (a) download, copy (for internal purposes only) and share this Material with your employees and consultants for study purposes, and (b) utilize the Material for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, Compliant Products, in all cases subject to the conditions set forth in this Agreement and any relevant patent and other intellectual property rights of third parties (which may include members of HL7). No other license, sublicense, or other rights of any kind are granted under this Agreement.

Please see <http://www.hl7.org/legal/ippolicy.cfm> for the full license terms governing the Material.

Record of Changes

Date	Version	Description	By
12/29/2006	0.1	Draft version	David Staggs
12/29/2006	0.2	Quality Assurance Review/Revision	Craig Winter
01/19/2007	0.3	Updates from HL7 CCOW TC meeting	David Staggs
01/22/2007	0.4	Quality Assurance Review/Revision	Craig Winter
02/20/2007	0.5	Incorporated revisions by Rob Seliger	David Staggs
02/27/2007	0.6	Incorporated revisions by CCOW TC	David Staggs
02/27/2007	0.7	Quality Assurance Review/Revision	Craig Winter
04/25/2007	0.8	Incorporated revisions by Ed Coyne	David Staggs
09/18/2007	0.9	Incorporated comments from CCOW TC review	David Staggs
11/13/2007	1.0	Edits in preparation for balloting	David Staggs
1/16/2008	1.1	Edits to reconcile comments from CCOW Ballot	David Staggs

Table of Contents

<u>Section</u>	<u>Page</u>
1 Introduction	1
1.1 Identification	1
1.2 Overview	1
1.3 Terms	2
1.4 Acronyms	3
2 TOE Description.....	4
3 Security Environment.....	6
3.1 Threats	6
3.1.1 CCOW-Specific Threats.....	6
3.1.2 Residual Risk	8
3.2 Organizational Security Policies.....	8
3.3 Security Usage Assumptions	8
3.3.1 Configuration Assumptions	9
3.3.2 Physical Assumptions	9
3.3.3 Personnel Assumptions	9
3.3.4 Connectivity Assumptions	9
4 Security Objectives	10
4.1 CCOW-specific IT Security Objectives.....	10
5 Functional Requirements	13
5.1 CCOW-Specific Functional Requirements	13
6 Rationale	17
6.1 Security Objectives Rationale	17
6.1.1 Complete Coverage - Threats	17
6.2 Security Requirements Rationale.....	19
6.2.1 Complete Coverage - Objectives	20
6.2.2 SFR descriptions	20

List of Figures

<u>Figure</u>	<u>Page</u>
Figure 1: CCOW TOE Architecture	5

List of Tables

<u>Table</u>	<u>Page</u>
Table 1: Mapping of Threats to Security Objectives	17
Table 2: Mapping of Functional Components to Security Objectives	20
Table 3: Descriptions of Security Functional Requirements	20

Preface

This document is intended for use with a Protection Profile conforming to the Common Criteria for Information Technology Security Evaluation (CCMB-2005-07-001), aligned with ISO/IEC 15408:2005 (October, 2005) at Evaluation Assurance Level 3. It was produced to address a need to improve the clinical sign-on process to provide both efficiency and security. It contains functionality specific to programs that are used for authenticating computer system users and which also implement the CCOW standard for context sharing, as promulgated by the Health Level 7 international standards development organization. More specifically, this protection package describes CCOW-specific functional security requirements required for a CCOW-compliant application. The CCOWAUTH protection package can be combined with this protection package to describe CCOW-specific functional security requirements required of an application designated as a user authentication CCOW-compliant application. CCOW-specific functional security requirements required of a CCOW-compliant context manager are described in the CCOWCM protection package.

Foreword

This document, *CCOW Application Protection Package*, is issued by the Health Level Seven (HL7) standards development organization. This Protection Package is based on the *HL7 Context Management ("CCOW") Standard: Technology- and Subject-Independent Component Architecture* Version 1.5, dated May 2004 (further referred to as *CCOWSpec*).

This Protection Package is in conformance with the requirements of the Common Criteria for Information Technology Security Evaluation (CC v3.0). A Protection Package is defined as:

A package is a named set of security requirements. A package can be a functional package and contain only Security Functional Requirements (SFRs). A package can be an assurance package and contain only Security Assurance Requirements (SARs). Mixed packages containing both SFRs and SARs are not allowed. A package can be defined by any party and is intended to be reusable. To this goal it should contain requirements that are useful and effective in combination. [...] Packages are used in the construction of larger packages, [Protection Profiles] PPs and [Security Targets] STs (*CC v3.0 §8.2*).

The functionality presented in this Protection Package may also be referenced from a Protection Profile as assignable criteria. The concept of assignable criteria and test steps was introduced by the CCHIT in 2006:

Assignable Criteria and corresponding Assignable Test Steps represent functions that may, at the vendor's option, be fulfilled by components external to the vendor's EHR product, such as third-party software, operating systems, hardware, or a network. For items externally Assigned by the vendor, compliance can be demonstrated by supplying suitable documentation and self-attestation. (*Certification Handbook; Ambulatory EHR Products 2006, Ver.1.2, May 1, 2006*)

Alternatively, authors may use this document as a guide for adding CCOW specific security functional requirements directly to their Protection Profile. Further information, including the status and updates of the Common Criteria, can be found on the Internet at <http://www.niap-ccevs.org/cc-scheme/>.

Acknowledgements

This Protection Package is based on the joint efforts of the HL7 CCOW Technical Committee and the HL7 Security Technical Committee. Special appreciation is owed to Dr. Ed Coyne for his contributions to the initial draft of this document.

1 Introduction

This document collects functionality that can be referenced or delegated from a parent Protection Profile that describes a target of evaluation implementing the CCOW standard. This section contains document management and overview information similar to that necessary to allow a Protection Profile to be registered through a Protection Profile Registry. The identification below provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference this document. The overview summarizes this document in narrative form and provides sufficient information for a potential user to determine whether this document is of interest. The overview can also be used as a stand-alone abstract for catalogues and registers.

1.1 Identification

Title: CCOW Application Protection Package (CCOWAPP)

Registration: Health Level 7

Keywords: Clinical Context Object Workgroup, CCOW, health information protection, context management

1.2 Overview

This Common Criteria (CC) CCOW Application Protection Package, hereafter called CCOWAPP, specifies a set of security functional requirements for access to health information in a clinical environment from a clinical application. This effort was provided to allow an application Protection Profile to more easily include CCOW functionality by referencing portions of this Protection Package. In the envisioned system, the CCOWAPP conformant Application Target of Evaluation (TOE) will interact with a CCOW context manager that supports the maintenance of patient context and user context across applications.

The CCOW Application TOE working in conjunction with a CCOW context manager will provide a patient context service that will synchronize access with medical information systems as a user simultaneously accesses various applications to view and record patient data from a single clinical desktop.

This protection package can be combined with the CCOWAUTH protection package to describe functional security requirements required of an application designated as a CCOW user authentication application. User authentication is not covered in the CCOWAPP.

The security functional requirements in this document provides for a level of protection that is appropriate for an assumed non-hostile and well managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. Reference to this Protection Package is not intended for Protection Profiles in which protection is required against determined attempts by hostile and well-resourced attackers to breach system security. The CCOWAPP does not fully address the threats posed by system development or administrative