



CCT MARK IA CLAIMS DOCUMENT (ICD) Ultra Electronics Datel

**Syntaxis Shared Collaborative Working Environment
Service**

Version 2.7

VENDOR DETAILS	
Ultra Electronics Datel	
1 Chain Caul Way, Ashton on Ribble, Preston, PR2 2YL	
Telephone Number:	01772 325 200
Vendor Website:	www.ultra-datel.com
Vendor Contact Email:	phil.clayton@ultra-datel.com

CERTIFICATE DETAILS	
CCT Mark Certificate Number	2007/06/0023
CCT Mark Awarded	28/06/2007
CCT Mark Award Expires on	27/06/ 2008
ICD Issue Date	28/06/ 2007

TABLE OF CONTENTS

1	INTRODUCTION	3
1.1	Background	3
1.2	Objectives.....	3
1.3	Purpose of Document.....	3
1.4	Structure.....	3
2	SERVICE DESCRIPTION	4
2.1	Service Identification	4
2.2	Service Overview.....	4
2.3	Usage Assumptions.....	9
3	SECURITY CLAIMS FOR THE IA SERVICE.....	11
3.1	Claims Statements	11
3.2	Existing Assurance Certificates	14
	Annex A : Abbreviations.....	15
	Annex B : Glossary	16
	Annex C : Marketing Statement	17

LIST OF FIGURES

Figure 1 - Syntaxis Overview	7
------------------------------------	---

LIST OF TABLES

Table 1 - IA Claims.....	11
Table 2 - Existing Assurance Certificates.....	14

1 INTRODUCTION

1.1 Background

This document outlines the Information Assurance (IA) claims made by Ultra Electronics Datel in regard to the suitability of the Syntaxis Shared Collaborative Working Environment (SCWE) Service for use by the UK Public Sector.

1.2 Objectives

The objectives of this ICD are to provide:

- An overview of the Syntaxis SCWE Service, detailing its functionality and architecture of the service;
- The security claims for the Syntaxis SCWE Service as tested under the CCT Mark Scheme; and
- A test approach setting out how the claims will be tested.

1.3 Purpose of Document

This document is the ICD for Syntaxis SCWE Service.

This ICD is the baseline document for the CCT Mark claims testing process of Syntaxis SCWE Service.

1.4 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains the introductory material;
- Section 2 contains the description of the services provided by Syntaxis SCWE Service and all the information related to the security of the Syntaxis SCWE Service;
- Section 3 details the security claims that are being made for the service;

2 SERVICE DESCRIPTION

2.1 Service Identification

Product Name:	Syntaxis SCWE Service https://www.syntaxis.r.mil.uk (Only accessible from RLI connected machines) https://www.syntaxis.uk.com (Internet connection requiring client certificate) https://www.syntaxis.gse.gov.uk (Only accessible from the GSi)
Version:	Syntaxis SCWE Service v2.7 (UED/CRUSO/BD/138)

Client Platform

Operating System / Version	Browser / Version
MS Windows XP Professional (SP2)	MS Internet Explorer 6.2 (SP2)

Period of Assessment: 12months (13/05/2006 to 12/06/2007)

2.2 Service Overview

Syntaxis is a secure web-based Shared Collaborative Working Environment (SCWE) used by the UK Public Sector to process information assets up to and including RESTRICTED.

Syntaxis was developed as a result of many years knowledge and experience in the delivery of SCWE Services. Syntaxis provides the UK Public Sector and their Partners with simple, secure and cost effective collaboration services using browser-based access from any permitted device and location.

The Syntaxis SCWE Service is accessible from the Government Secure Intranet (GSi), Restricted LAN Interconnect (RLI), and the Public Internet. The confidentiality and integrity of information assets entering and leaving Syntaxis are protected using commercial software encryption.

The collaborative application provided within Syntaxis is eRoom, which is a Commercial-off-the-Shelf (COTS) product.

Within the Syntaxis SCWE Service, groups of users wishing to collaborate are created within a community. The service is able to accommodate numbers of communities, and is able to ensure that people and information remain within their respective communities.

Indeed, the users within any particular community will be unaware of the existence of any other community. New communities can be deployed within 24hrs.

Within each community a number of organisations may be present. The service requires each organisation to nominate a sponsor, who will have delegated user administration privileges on behalf of their organisation. This enables a sponsor to create users, delete users and modify the contact details of their users, to reset passwords and also create additional sponsors on behalf of their organisation.

Key collaboration features include:

- document management capability - members of the extended enterprise (geographical business partners representing different organisations that have no common sharing ability) can gain access to current document versions and all previous versions;
- user defined "work spaces" (collaboration areas which can be created by authorised users to meet specific needs of the business);
- approval workflow – a facility which enables a simple process of reviewing and approving documents;
- a project planning tool – allows date plans to be shared and managed across a team or programme;
- database facility – a fully customisable user defined database for milestones, issues, contacts or other structured project information;
- team calendar – with month, week and list views, recurring events;
- user poll – a question is presented with possible responses (as users vote, the results are automatically tabulated and displayed);
- task tracker – a facility that enables actions and tasks to be created and monitored;
- discussion forum – facilitates a structured debate, for example against documents under review;
- quick search capability – locates matching items in all of the collaborative facilities and adheres to access control settings; and
- chat facility – enables users to communicate in real-time with others who are logged onto 'work spaces'.

The security of the environment is maintained through the effective application of UK Public Sector IA as defined by the Manual of Protective Security.

2.2.1 Security Architecture

When data is transmitted over the internet the Syntaxis SCWE Service protects the confidentiality of information in transit through the use of good practice commercial software encryption.

The premises from which the Syntaxis service operates are approved to protect information assets protectively marked up to and including RESTRICTED.

The key features of the security architecture include:

- physical security - the service delivery platform is protected to the standards required for the protection of RESTRICTED information assets;
- X.509 user-identity binding certificates - used over the Internet as an additional factor of authentication;
- authentication – each user is required to uniquely authenticate with the system using a username and password;
- single sign on – users only require to log on with one username and password to use all applications;
- session management – at the commencement of each session, a one-time session credential is provided. Session credentials are invalidated after a period of inactivity to ensure that users do not neglect to log off;
- access controls – two levels of access control are implemented:
 - community level – the service can support multiple communities of users. Information sharing is only possible between members of the same community;
 - access to information stored within a community is configurable by the person who uploads the information;
- malware controls – effective malware controls are maintained by the use of industry standard malware control software.
- audit –user transactions (log-on, view/download/read, upload/create/modify) are logged by the system, detailing for each transaction;
 - The identity of the Operator making the transaction
 - The data object involved in the transaction
 - The nature of the transaction (log-on, view/download/read, upload/create/modify)
 - The date and time of the transaction.

The security architecture has been verified through the use of independent IT health checks.

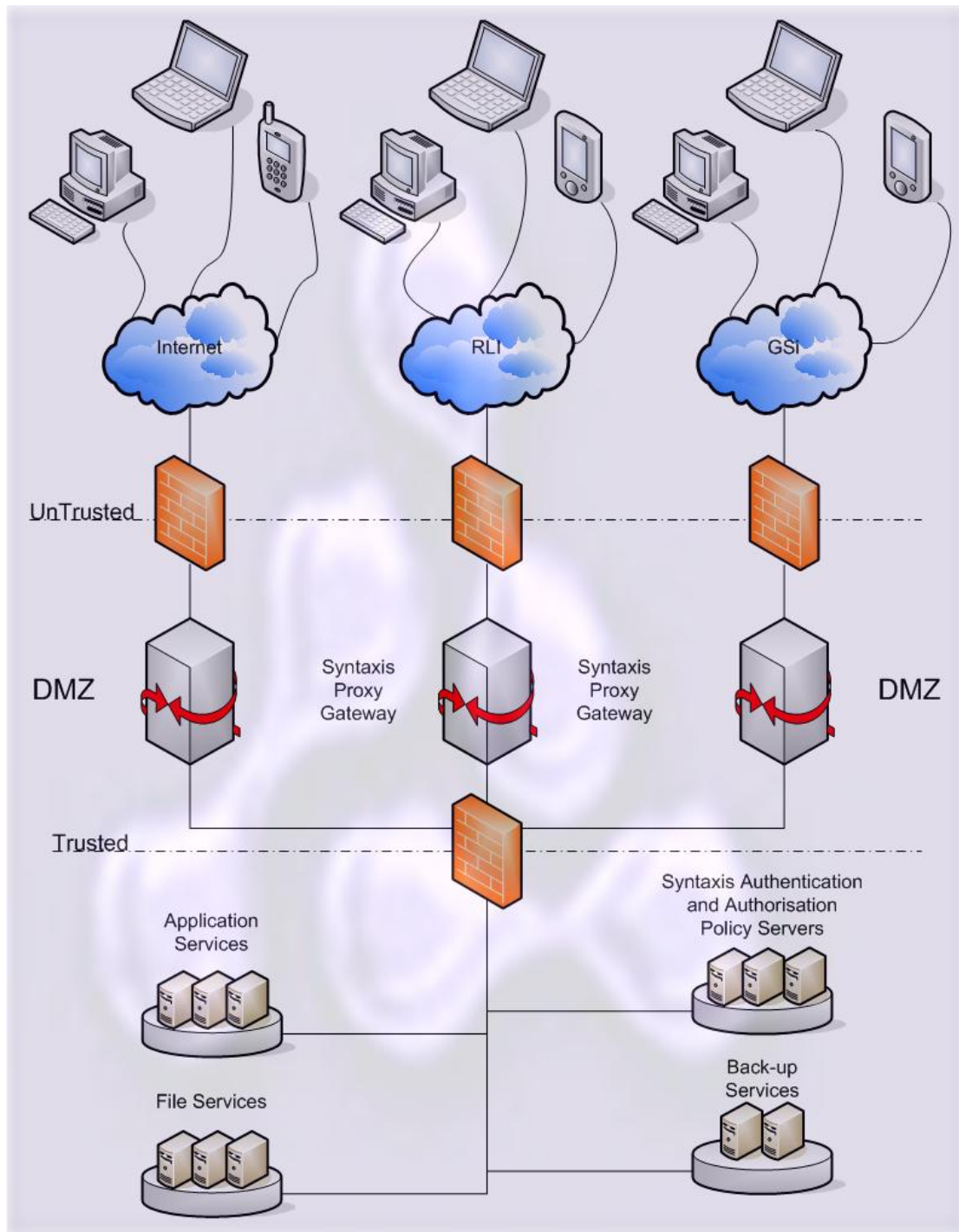


Figure 1 - Syntaxis Overview

2.2.2 Hardware Requirements

As Syntaxis is designed to be accessible using a web browser, any computing device supporting MS IE6 SP2 can be used.

For the purposes of testing, the platform shall be Windows XP Professional SP2.

2.2.3 Software Requirements

Syntaxis can be used by any version of Internet Explorer (IE), however only IE6 SP2 is fully supported. No additional software is required to run any applications, however, as with any internet-based product, technical factors such as bandwidth, network configurations, and browser settings can affect the speed and accessibility.

Users who access Syntaxis via the Internet are required to be in possession of an X.509 identity-binding certificate in order to gain access to the service. These certificates are issued by Ultra Electronics Datel as part of the service.

2.2.4 Out of Scope

The service will operate on operating systems and browsers other than those detailed at paragraph 2.1, however such combinations are outside the scope of this assessment.

Greater desktop integration can be achieved through the use of an optional plug-in; this is out of scope of this document.

In addition to shared collaborative facilities the Syntaxis environment can be tailored to host additional applications to meet customer's specific collaboration requirements. Examples of applications hosted include:

- Product Data Management;
- Document Management;
- Requirements Management; and
- Risk Management.

Applications that can be hosted include web based applications and client/server applications through the use of Citrix based technologies.

These additional facilities are not included in the CCT Mark testing of the service.

2.3 Usage Assumptions

2.3.1 Assets

Assets which are to be protected include HMG and corporate files and information held within the system.

2.3.2 Threat Scenario

Threats to assets which are countered are:

- T1** physical access to service components by unauthorised personnel;
- T2** network and application level attacks originating from external networks and/or the Internet;
- T3** electronic attack from unknown individuals or organisations;
- T4** unauthorised access to sensitive information by authenticated users;
- T5** introduction of malicious code on to Syntaxis by end users, and subsequently transfer on to end user computers and/or networks;
- T6** eavesdropping on communications;
- T7** users failing to logout from untrusted environments; and
- T8** negligent or malicious usage by the end user leading to compromise of the Confidentiality and Integrity of information hosted by the service.

2.3.2.1 Expected Operational Environment

It is expected that Syntaxis SCWE will be employed with an infrastructure that will enable users to access web based files and applications. It is also expected that Syntaxis will be used by Government bodies, organisations and users with a requirement for secure collaboration.

Syntaxis allows sensitive information to be shared across organisationally and geographically dispersed communities of interest.

2.3.2.2 Organisational Security Policies

To utilise the Syntaxis SCWE Service, user organisations will be required to conform security standards such as those defined by; the Manual of Protective Security; Joint Service Publication 440; or ISO/IEC 17799, and abide by the Code of Connection detailed in Code of Connection for Syntaxis Secure Collaborative Working Environment UED/CRUSO/CO/899) published 3rd April 2007.

2.3.2.3 Security Requirements on the Environment

Service Provider

- staff are security cleared to a minimum of Security Check (SC) level;
- staff are suitably trained to carry out their duties;
- Syntaxis operates in a secure hosting environment; and
- all communications over the Internet are secured.

Client End Users

The following assumptions characterise the operational security requirements of the expected environment.

- one or more competent persons will be nominated to perform the role of Sponsor for each organisation within the community, and will have delegated user administration responsibilities within the system;
- organisations shall commit to protecting the confidentiality of information processed by the system; and
- users of the service are trusted to follow the guidance provided for its secure operation.

3 SECURITY CLAIMS FOR THE IA SERVICE

3.1 Claims Statements

Table 1 - IA Claims

Claims Reference	Claim
	Physical Security
CS1	The premises from which the system is operated are protected to the standards required for the protection of assets protectively marked up to and including 'RESTRICTED'.
	Encryption
CS2	The confidentiality and integrity of information assets entering and leaving Syntaxis are protected using good practice, commercial software encryption and the system is used to process information assets with the protective marking up to Restricted.
	Authentication Support
CS3	X.509 user-identity binding certificates are used over the Internet as an additional factor of authentication.
CS4	Each user is required to uniquely authenticate with the system using a username and password.
CS5	Users only require to logon with one username and password to use all the applications appropriate to their role.
CS6	To ensure users logoff, session credentials are invalidated after a period of 8 hours.
	Management
CS7	Within each community a number of organisations may be present. The service requires each organisation to nominate a sponsor, who will have delegated user administration privileges on behalf of their organisation. This enables a sponsor to create users, delete users and modify the contact details of their users, to reset passwords and also create additional sponsors on behalf of their organisation.

Claims Reference	Claim
CS8	<p>Nominated Sponsors have administration privileges that enable them to manage the X.509 certificates (used over the Internet as an additional factor of authentication) provided by Syntaxis. These management capabilities include;</p> <ul style="list-style-type: none"> • Downloading the Certifying Authority's certificate. • Generating a new user certificate and its associated password. • Replacing a user certificate and its associated password. • Revoke (remotely invalidate) a user's certificate. • Download (or optionally download and install) a user's certificate.
	Collaborative Capabilities
CS9	The service can support multiple communities of users. Information sharing is only possible between members of the same community.
CS10	Access to information stored within a community is configurable by the person who uploads the information.
CS11	<p>The eRoom application provides the following collaborative capabilities:</p> <ul style="list-style-type: none"> • simple documentation management capability with version control; • user defined collaboration areas; • approval workflow; • a project planning tool; • database facility; • team calendar; • user polling; • task tracking; • discussion forums; • quick search capability; and • chat facilities.

Claims Reference	Claim
	Accessibility
CS12	Syntaxis is accessible by users based on the GSI, RLI and Internet.
CS13	The Syntaxis service delivery system's security mechanisms are subjected to regular IT health checks. by an independent provider of security services.
CS14	Communities can be deployed within 24hrs.
CS15	Syntaxis allows collaborative working between members of the extended enterprise (geographical business partners representing different organizations that have no common sharing ability).
	Audit
CS16	<p>Transactions with the Syntaxis SWE service are logged for analysis if required.</p> <p>For each transaction the logs contain details of;</p> <ul style="list-style-type: none"> - The identity of the Operator making the transaction - The data object involved in the transaction - The nature of the transaction (log-on, view, upload, download, (log-on, view/download/read, upload/create/modify) - The date and time of the transaction.
	Malware Controls
CS17	Malware controls are maintained by the use of industry standard malware control software from one of the industry leading vendors. Anti Virus updates are performed on a weekly basis.
CS18	Malware controls are configured to perform a full system scan every day.
CS19	Files uploaded to the system are scanned by the Malware control Software and any that are identified as containing a virus are subject to a cleaning routine and if that fails immediately deleted.

3.2 Existing Assurance Certificates

Product	Certificate
Health check reports	9/12/2004, 6/1/06 and 19/4/2007

Table 2 - Existing Assurance Certificates

Annex A : Abbreviations

CCT	CSIA Claims Tested
COTS	Commercial off the Shelf
CSIA	Central Sponsor for Information Assurance
GSi	Government Secure Intranet
HMG	Her Majesty's Government
IA	Information Assurance
ICD	IA Claims Document
IE6	Internet Explorer v6
IEC	International Electro-technical Commission
ISO	International Standards Organisation
IT	Information Technology
LAN	Local Area Network
MS	Microsoft
RLI	Restricted LAN Interconnect
SC	Security Check
SCWE	Secure Collaborative Working Environment
SP2	Service Pack 2
UED	Ultra Electronics Datel
UK	United Kingdom

Annex B : Glossary

X.509	digital certificate used for authentication
IT Health Check	A passive assessment of the vulnerability of a system to public domain exploits.
SCWE	<p>The following applications or services are often (but not exclusively) considered as elements of a SCWE.</p> <ul style="list-style-type: none">• Instant Messaging• Application sharing• Collaborative workspace• Collaborative Document Management• Workflow Management.
Malware	general term used to describe any sort of malicious software such as viruses, worms, Trojans, etc.

Annex C : Marketing Statement

Ultra Electronics Datel recognises that teamworking is crucial to many modern enterprises. Teams are often geographically dispersed and reliant on modern technology for communication. With time being one of today's most precious resources; there's a requirement for teams to share information and knowledge safely and securely in real time.

By use of the Syntaxis product, Ultra Electronics Datel provides a Secure Collaborative Working Environment to a wide cross-section of Industry and Government customers, delivering real time collaborative working.

Syntaxis not only enables joint Government and/or Industry to communicate freely on engagements, but allows teams to share materials and contribute to work-in-progress, providing project stakeholders with the right information at the right time in the right place.

Accessible from the Internet, the RLI and the GSI, Syntaxis provides the flexibility needed for all stakeholders, regardless of location, to contribute.