National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Public Key-Enabled Application Family of Protection Profiles, Version 2.5

Report Number: CCEVS-VR-02-0031
Version: 1.1
Dated: 12 December 2002

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Paul A. Olson
National Security Agency
Ft. George G. Meade, Maryland

Common Criteria Testing Laboratory

Gary Grainger
Kris Rogers
CygnaCom Solutions
McLean, Virginia

TABLE OF CONTENTS:

1 Executive Summary

The Public Key Enabled Application Family of Protection Profiles, Version 2.5, was evaluated against the requirements for Protection Profiles in the Common Criteria for Information Technology Security Evaluation, ISO Standard 15408. The evaluation was conducted in accordance with the standards and procedures of the Common Criteria Evaluation and Validation Scheme, under the National Information Assurance Partnership program. The method employed in the evaluation was defined in chapter 3, "PP evaluation" of the Common Evaluation Methodology for Information Technology Security, Version 0.6. All APE requirements were met.

This family of PPs defines security requirements for a PK enabled application and its environment. An application is PK enabled if it:

- Securely manages keys, trust anchors, and certificates.
- Uses one or more of the security services supported by the DoD PKI by accepting and processing a DoD X.509 digital certificate.
- Is able to obtain relevant certificates and revocation data.
- Checks each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance, including checking for revocation.
- Has access to accurate and reliable time in order to verify the dates on certificates, revocation data, and application data.
- Correctly operates with the Common Access Card (CAC) or another DoD approved "hard token".
- Collects, stores and maintains the data required to support digital signature verification in the future.
- Is able to automatically select from multiple private decryption keys if it performs public key based decryption.

A PKE application must operate correctly with the DoD PKI. The Defense Information Systems Agency (DISA), Joint Interoperability Test Center (JITC) has developed the "Department of Defense Public Key Infrastructure Interoperability Master Test Plan Version 1.2, dated November 2001". DISA has determined that a PK-Enabled application operates correctly with the DoD PKI if the application successfully completes this test protocol. In this family of PPs, application is synonymous with Target of Evaluation (TOE).

This family of PPs defines different PK services. Thousands of possible PPs may be defined depending upon the combination of functional packages and the EAL chosen to meet the requirements of the application. Many functional requirements in the PPs represent extensions to the Common Criteria (CC), because the CC does not provide requirements for the X.509 processing rules that are critical to this family of PPs.

The PK-Enabled Application Family of Protection Profiles defines

- a base set of functional requirements for all PKE Applications
- a set of functional requirements for the environment for the application
- 15 packages of additional functionality. The packages define requirements for any of several PKE services (e.g., CPV Name Constraints, PKI Signature Verification).
- Assurance requirements for EAL 3 with augmentation
- Assurance requirements for EAL 4 with augmentation
- Instructions for assembling these requirements into a single PP that expresses the PP user's security requirements.

All PPs in this family are named with the form:

USMC PKE PP with <packages included in the PP, listed in the order in which they appear in the PP> **at EAL** <3 or 4, depending on the EAL selected> **with augmentation**

This assures that PPs from this family have unique names.

Applicable Interpretations

All Common Criteria Interpretations with an effective date on or before 20 June 2002 were considered as applicable to this document. This family of Protection Profiles was found compliant with these interpretations.

2 Identification

Name: Public Key-Enabled Application Family of Protection Profiles
Date: 31 October 2002
Version: 2.5
Identity of the Developer: Jean Petty, Entrust CygnaCom and Santosh Chokhani, Orion Security Solutions, Inc.
Identity of the Evaluator: Kristina Rogers and Gary Grainger, Entrust CygnaCom
Evaluation Completion Date: November 19, 2002
Evaluation Standard: Common Criteria for Information Technology Security Evaluation, Version 2.1

3 Assumptions and Clarification of Scope

Products compliant with the requirements in one or more of the PPs in this family are expected to counter the threat of users masquerading as other users or Certificate Authorities, however performed, and the misuse of certificates and control messages. It is assumed that compliant products

- Are controlled by trustworthy personnel within physically protected facilities.
- Are properly installed and configured with a FIPS 140-compliant cryptographic module and an accurate time clock.
- Have certificate and certificate revocation information available to them.

In addition, there are constraints in the development of this Protection Profiles family due to the use of packages:

1. Each package is complete, i.e., each package contains a name, TOE Description, threats, organization security policy (if applicable), secure usage assumptions (if applicable), security objectives for the TOE (if applicable), security objectives for the environment (if applicable), security functional requirements for the TOE (if applicable), IT security functional requirements for the environment (if applicable), non-IT security functional requirements for the environment (if applicable), security assurance requirements, security objectives rationale, security requirements rationale, dependencies rationale, and strength of function rationale. In other words, the package has all of the components of a PP.
2. A dependency rationale points to other packages to satisfy some of the requirements. Note that dependencies are specifically identified for packages both in Section 2.3 and in Section 5.3 of the PKE PP Family document. Also, the requirement that dependencies must be included is repeated in Section 2.3 and in Section 5.3.
3. Some material is included in a package by reference. For example, if assurance requirements and strength of function requirements are common to some or all packages, it is sufficient to include them only once as long as it is clear which packages are applicable.
4. From the TOE description, it is obvious that the security functionality provided by each package is different from functionality provided by other packages under evaluation.
5. The threats for each package are different from the threats for other packages. This means:
    a. A threat name appears in only one package, and
    b. Each threat description is distinct.

6. The objectives for each package are different from the objectives for other packages. This means:
    a. An objective name appears in only one package, and
    b. Each objective description is distinct.
7. The security functional requirements and security assurance requirements for all of the packages have the same label if and only if they are identical.
8. The authors describe the algorithm for naming the various composite PPs and show that they result in unique name for each possible composite PP.

Package Format

The PP Family comprises 15 functional packages, each with its own corresponding threats and objectives:

1. Certification Path Validation – Basic Package
2. Certification Path Validation – Basic Policy Package
3. Certification Path Validation – Policy Mapping Package
4. Certification Path Validation – Name Constraints Package
5. PKI Signature Generation Package
6. PKI Signature Verification Package
7. PKI Encryption using Key Transfer Algorithms Package
8. PKI Encryption using Key Agreement Algorithms Package
9. PKI Decryption using Key Transfer Algorithms Package
10. PKI Decryption using Key Agreement Algorithms Package
11. PKI Bases Entity Authentication Package
12. Online Certificate Status Protocol Client Package
13. Certificate Revocation List Validation Package
14. Audit Management Package
15. Continuous Authentication Package

The evaluator found the package names and descriptions are consistent in the PKE PP family.

4 Results of Evaluation

The Public Key-Enabled Protection Profile (PKE PP) was evaluated against the following Common Criteria (CC) Part 3 components using Version 1.0 of the Common Evaluation Methodology for Information Technology Security (CEM):

- APE_DES.1,
- APE_ENV.1,
- APE_INT.1,
- APE_OBJ.1,
- APE_REQ.1,
- APE_SRE.1, and
- Interpretations.

Table 4-1 summarizes the evaluation results.

Table 4-1 – Evaluation Results

Component	Work Unit	Verdict
APE_DES.1		**Pass**
APE_DES.1.1E		Pass
APE_DES.1.2E		Pass
APE_DES.1.3E		Pass
APE_ENV.1		**Pass**
APE_ENV.1.1E		Pass
APE_ENV.1.2E		Pass
APE_INT.1		**Pass**

APE_INT.1.1E		Pass
APE_INT.1.2E		Pass
APE_INT.1.3E		Pass
APE_OBJ.1		**Pass**
APE_OBJ.1.1E		Pass
APE_OBJ.1.1E		Pass
APE_REQ.1		**Pass**
APE_REQ.1.1E		Pass
APE_REQ.1.2E		Pass
APE_SRE.1		**Pass**
APE_SRE.1.1E		Pass
APE_SRE.1.2E		Pass
Interpretations		**Pass**
Common Criteria		Compliant
NIAP CCEVS		N/A

APE_DES.1 Protection Profile, TOE description, Evaluation requirements

Dependencies:

APE_ENV.1 Protection Profile, Security environment, Evaluation requirements
APE_INT.1 Protection Profile, PP introduction, Evaluation requirements
APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements
APE_REQ.1 Protection Profile, IT security requirements, Evaluation Requirements

Developer action elements:

APE_DES.1.1D The PP developer shall provide a TOE description as part of the PP.

Content and presentation of evidence elements:

APE_DES.1.1C The TOE description shall as a minimum describe the product type and the general IT features of the TOE.

Evaluator action elements:

APE_DES.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
APE_DES.1.2E The evaluator shall confirm that the TOE description is coherent and internally consistent.
APE_DES.1.3E The evaluator shall confirm that the TOE description is consistent with the other parts of the PP.

Applicable Features:

The evaluator reviewed the TOE Description and found

- The description presents the product type as a PK Enabled Application., as defined in the Section 1, Executive Summary, above

- The description is internally consistent, and it is coherent to its target audience. It defines

- a PKE Application
- the approach (i.e., the packages)
- how to assemble packages into a full PP
- how this PP family was evaluated
- TOE Definition
- Assurance requirements summary

The description was compared one-to-one with all of the other sections of the PP Family and found that no other section contradicted or altered any statement in the TOE Description.

APE_ENV.1 Protection Profile, Security environment, Evaluation requirements

Dependencies:

No dependencies.

Developer action elements:

APE_ENV.1.1D The PP developer shall provide a statement of TOE security environment as part of the PP.

Content and presentation of evidence elements:

APE_ENV.1.1C The statement of TOE security environment shall identify and explain any assumptions about the intended usage of the TOE and the environment of use of the TOE.

APE_ENV.1.2C The statement of TOE security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment.

APE_ENV.1.3C The statement of TOE security environment shall identify and explain any organisational security policies with which the TOE must comply.

Evaluator action elements:

APE_ENV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

APE_ENV.1.2E The evaluator shall confirm that the statement of TOE security environment is coherent and internally consistent.

Applicable Features:

All assumptions and threats were found to be coherent to the intended audience and internally consistent. They were compared one-to-one with all other assumptions/threats and they did not conflict with one another. All threats are labeled with a name of the format "T.<name>" and assumptions are labeled with a name of the format "A.<name>". Each package has its own list of threats, which follow the constraints defined above. There is one list of assumptions corresponding to the base set of requirements, hence all assumptions apply to all PPs in this family.

There are no organizational security policies, hence the APE_ENV.1.3C requirement may be considered satisfied.

APE_INT.1 Protection Profile, PP introduction, Evaluation requirements

Dependencies:

APE_DES.1 Protection Profile, TOE description, Evaluation

requirements

APE_ENV.1 Protection Profile, Security environment, Evaluation requirements

APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

APE_REQ.1 Protection Profile, IT security requirements, Evaluation requirements

Developer action elements:

APE_INT.1.1D The PP developer shall provide a PP introduction as part of the PP.

Content and presentation of evidence elements:

APE_INT.1.1C The PP introduction shall contain a PP identification that provides the labelling and descriptive information necessary to identify, catalogue, register, and cross reference the PP.

APE_INT.1.2C The PP introduction shall contain a PP overview which summarises the PP in narrative form.

Evaluator action elements:

APE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

APE_INT.1.2E The evaluator shall confirm that the PP introduction is coherent and internally consistent.

APE_INT.1.3E The evaluator shall confirm that the PP introduction is consistent with the other parts of the PP.

Applicable Features:

The evaluator found that the PP Introduction provides a PP overview in narrative form. The PP overview states that the family of PPs "describes the Information Technology (IT) security requirements for a PKE Applications, based on the X.509 standard (see references below), integrated into computing platforms or systems."
The PP Overview also provides an overview of the security functionality and important features of the PP such as the use of packages and explicitly stated requirements.

The evaluator found the PP introduction is understandable by the target audience, is internally consistent, and is consistent with the other parts of the PP.

The evaluator examined the PP naming scheme to determine whether the scheme uniquely and unambiguously names each possible PP in the PP family. The analysis included applying the naming algorithm to sample cases, one of which consisted of a PP containing all the packages, and verifying that each case resulted in a unique, meaningful, and unambiguous name. In all cases the algorithm generated such a name.

APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

Dependencies:

APE_ENV.1 Protection Profile, Security environment, Evaluation

requirements

Developer action elements:

APE_OBJ.1.1D The PP developer shall provide a statement of security objectives as part of the PP.

APE_OBJ.1.2D The PP developer shall provide the security objectives rationale.

Content and presentation of evidence elements:

APE_OBJ.1.1C The statement of security objectives shall define the security objectives for the TOE and its environment.

APE_OBJ.1.2C The security objectives for the TOE shall be clearly stated and traced back to aspects of the identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE.

APE_OBJ.1.3C The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats not completely countered by the TOE and/or organisational security policies or assumptions not completely met by the TOE.

APE_OBJ.1.4C The security objectives rationale shall demonstrate that the stated security objectives are suitable to counter the identified threats to security.

APE_OBJ.1.5C The security objectives rationale shall demonstrate that the stated security objectives are suitable to cover all of the identified organisational security policies and assumptions.

Evaluator action elements:

APE_OBJ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

APE_OBJ.1.2E The evaluator shall confirm that the statement of security objectives is complete, coherent, and internally consistent.

Applicable Features:

The evaluator reviewed the statement of security objectives and found that that the statement of security objectives defines the security objectives for the TOE and its environment.

Security objectives for the TOE appear in Sections 4.1 and 4.3 and use the naming convention of "O.*". Security objectives for the Environment appear in Section 4.2 and use the naming convention of "OE.*."

The TOE Description and IT Security Requirements explicitly allow ST authors to allocate some TOE requirements in the PP to the IT environment in a compliant ST. The introduction to Section 4.1 provides the ST author with guidance on re-labeling security objectives when the environment meets them.

PKE PP family Section 4.3 lists TOE security objectives by package, which clearly identifies the TOE objectives contained in each of the 15 packages. Security Objectives for the environment (IT and non-IT) are not attached to any one package, rather they apply to all PPs in this Family. PKE PP family Section 6.1.2 presents security objectives rationale by package for each of the 15 packages.

All security objectives for the TOE trace back to threats to be countered and assumptions to be supported. All security objectives for the environment trace back to assumptions. The rationale provided adequately justifies the tracing. There are no organizational security policies; therefore this work unit is not applicable and therefore considered to be satisfied.

The evaluator examined the statement of security objectives for clarity and understandability, internal consistency, and completeness. The evaluator found that the statement of security objectives was understandable by its target audience. It was also complete and internally consistent. In addition, the evaluator examined the packages for both duplicate security objective names and duplicate objective descriptions. The evaluator found the security objective names and descriptions to be distinct.

APE_REQ.1 Protection Profile, IT security requirements, Evaluation requirements

Dependencies:

APE_OBJ.1 Protection Profile, Security objectives, Evaluation requirements

Developer action elements:

APE_REQ.1.1D The PP developer shall provide a statement of IT security requirements as part of the PP.

APE_REQ.1.2D The PP developer shall provide the security requirements rationale.

Content and presentation of evidence elements:

APE_REQ.1.1C The statement of TOE security functional requirements shall identify the TOE security functional requirements drawn from CC Part 2 functional requirements components.

APE_REQ.1.2C The statement of TOE security assurance requirements shall identify the TOE security assurance requirements drawn from CC Part 3 assurance requirements components.

APE_REQ.1.3C The statement of TOE security assurance requirements should include an Evaluation Assurance Level (EAL) as defined in CC Part 3.

APE_REQ.1.4C The evidence shall justify that the statement of TOE security assurance requirements is appropriate.

APE_REQ.1.5C The PP shall, if appropriate, identify any security requirements for the IT environment.

APE_REQ.1.6C All completed operations on IT security requirements included in the PP shall be identified.

APE_REQ.1.7C Any uncompleted operations on IT security requirements included in the PP shall be identified.

APE_REQ.1.8C Dependencies among the IT security requirements included in the PP should be satisfied.

APE_REQ.1.9C The evidence shall justify why any non-satisfaction of dependencies is appropriate.

APE_REQ.1.10C The PP shall include a statement of the minimum strength of function level for the TOE security functional requirements, either SOF-basic, SOF-medium or SOF-high, as appropriate.

APE_REQ.1.11C The PP shall identify any specific TOE security functional requirements for which an explicit strength of function is appropriate, together with the

specific metric.

APE_REQ.1.12C The security requirements rationale shall demonstrate that the minimum strength of function level for the PP, together with any explicit strength of function claim, is consistent with the security objectives for the TOE.

APE_REQ.1.13C The security requirements rationale shall demonstrate that the IT security requirements are suitable to meet the security objectives.

APE_REQ.1.14C The security requirements rationale shall demonstrate that the set of IT security requirements together forms a mutually supportive and internally consistent whole.

Evaluator action elements:

APE_REQ.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

APE_REQ.1.2E The evaluator shall confirm that the statement of IT security requirements is complete, coherent, and internally consistent.

Applicable Features:

The PKE PP Family identifies all TOE security requirements that are drawn from Part 2 and Part 3 of the Common Criteria .

All PPs in this Family are either EAL3, augmented by ALC_FLR.1, or EAL4, likewise augmented. The PP naming algorithm clearly identifies the EAL selected for any possible PP.

The PKE PP Family's use of each Part 2 SFR and Part 3 SAR was compared against the text of the Common Criteria. Each reference to a TOE security functional requirement component is correct and each requirement was reproduced correctly. No package contains security assurance requirements.

The security requirements rationale sufficiently justifies that the statement of TOE security assurance requirements is appropriate for each PP in the family. The rationale provided was consistent with the guidance in the CC Part 3 Sections 6.2.3 and 6.2.4 and reflected consumer requirements.

There are no security assurance requirements for the IT environment. The PKE PP family identifies all security functional requirements for the IT environment.

All operations (assignments, refinements, selections, and iterations) were completed correctly. In addition, in accordance with the constraints, the evaluator examined the packages for duplicate requirements. The evaluator found no duplicate requirements in packages. All uncompleted operations on IT security requirements included in the PP were clearly identified.

The evaluator examined the developer's dependency analysis in Table 6.34 – Functional Requirements Dependencies. The evaluator found that an appropriate justification is given for each case where security requirement dependencies are not satisfied.

The evaluator checked the PP for a minimum strength of function requirement. The evaluator found that the family of PPs includes in minimum strength of function requirement of SOF-basic in Section 5.1.5, which applies to all packages. The SOF rationale states that the calculated attack potential is low, which confirms a minimum strength of function no more than SOF-basic. Thus, the rationale demonstrates SOF-basic is consistent with the objectives.

The family of PP identifies the specific TOE security functional requirements for which an explicit strength of function is appropriate, together with the specific metric.

The rationale traces each TOE security requirement back to at least one security objective for the TOE. There are three security requirements for the IT environment and each one traces back to a security objective for the IT environment. The rationale for each security objective for the TOE contains appropriate justification that the TOE security requirements are suitable to meet that security objective.

There are three security objectives for the IT environment: OE.Crypto, OE.PKI_Info, and OE.Time. For each of these security objectives, the justification in the rationale demonstrated that the security requirements for the IT environment are suitable to meet the objective. The remaining security objectives for the environment (OE.Authorized_Users, OE.Configuration, OE.Low, and OE.Physical_Security) are not IT objectives.

The evaluator performed a pair-wise review of the requirements to check that they were not inconsistent with each other. The review included all requirements for the packages taken together. The evaluator found that different IT security requirements are either clearly consistent or do not apply to the same types of events, operations, data, tests, etc. In either of these cases, no justification is needed.

The statement of IT security requirements was found to be coherent, complete, and internally consistent.

The functional requirements package guidance clearly identifies the functions covered by each package and the corresponding use of functional security requirements is consistent between packages. This included examining the packages for package dependencies and duplicate requirements. The guidance clearly explains the use of packages in general together with the base security functional requirements and requirements for the IT environment. The guidance identifies functions covered by each package and package dependencies.

In the course of successfully completing evaluator action elements APE_REQ.1.1E, APE_SRE.1.1E, and APE_SRE.1.2E, the evaluator found that the statement of IT security requirements is internally consistent.

APE_SRE.1 Protection Profile, Explicitly stated IT security requirements, Evaluation requirements

Dependencies:

APE_REQ.1 Protection Profile, IT security requirements, Evaluation requirements

Developer action elements:

APE_SRE.1.1D The PP developer shall provide a statement of IT security requirements as part of the PP.

APE_SRE.1.2D The PP developer shall provide the security requirements rationale.

Content and presentation of evidence elements:

APE_SRE.1.1C All TOE security requirements that are explicitly stated without reference to the CC shall be identified.

APE_SRE.1.2C All security requirements for the IT environment that are explicitly stated without reference to the CC shall be identified.

APE_SRE.1.3C The evidence shall justify why the security requirements had to be explicitly stated.

APE_SRE.1.4C The explicitly stated IT security requirements shall use the CC requirements components, families and classes as a model for presentation.

APE_SRE.1.5C The explicitly stated IT security requirements shall be measurable and state objective evaluation requirements such that compliance or noncompliance of a TOE can be determined and systematically demonstrated.

APE_SRE.1.6C The explicitly stated IT security \requirements shall be clearly and unambiguously expressed.

APE_SRE.1.7C The security requirements rationale shall demonstrate that the assurance requirements are applicable and appropriate to support any explicitly stated TOE security functional requirements.

Evaluator action elements:

APE_SRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

APE_SRE.1.2E The evaluator shall determine that all of the dependencies of the explicitly stated IT security requirements have been identified.

Applicable Features:

PKE PP family Section 5.3 lists TOE security functional requirements by package, which clearly identifies the TOE functional requirements contained in each of the 15 packages. Together with Table 5.1, this identifies the explicitly stated requirements in each package. There are two explicitly stated security requirements for the IT environment, FCS_CRM_FPS.1 and FDP_ITC_PKI_INF.1. Both requirements are identified as such.

The evaluator found that each explicitly stated IT security requirement uses the CC requirements components, families and classes as a model for presentation. Each explicitly stated IT security requirement was added to an existing CC class and given an appropriate extension. The functional components were defined to a comparable level of detail and broken down into individual functional elements. Operations were specified appropriately.

The justification for why each explicitly stated IT security requirement had to be explicitly stated states:

> "CC access control related components are not appropriate to express the certificate and revocation information (e.g., Certificate Revocation List (CRL), OCSP response, etc.) processing requirements and hence the Common Criteria Part 2 was extended to address the processing of certificates and revocation information."

No CC requirements in Part 2 were found to be adequate to express the X.509 functionality required.

Each explicitly stated requirement is measurable and states an objective evaluation requirement.

The functional security requirements rationale justifies the use of CC Part 3 assurance requirements based on the similarity between the explicitly stated functional requirements and CC Part 2 requirements and on the processing-oriented nature of the explicitly stated functional requirements. The security assurance requirements were found to be applicable and appropriate for supporting the explicitly stated requirements.

The evaluator examined each element of the explicitly stated components and found that all appropriate dependencies had been identified.

5 Evaluator Comments & Recommendations

The PKE PP family is complete, consistent, and technically sound. Each PP in the family should be suitable for use as a statement of requirements for evaluation of a public key-enabled application. Based on the analysis presented in Section 3, each PP in the PKE PP Family passes PP evaluation.

6 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, ISO Standard 15408.

[2] Public Key-Enabled Application Family of Protection Profiles, Version 2.5

[3] Public Key-Enabled Family of Protection Profiles V2.5 Evaluation Technical Report, Version 1.1, 5 November 2002, by Gary Grainger and Kristina C. Rogers, Cygnacom Solutions, Inc.