Digital Identity Technologies Department
Information Security Research Institute

Common Criteria certification pathways for threshold signature systems

Version 1.0

Michael Buckland, Peeter Laud, Sandhra-Mirella Valdma

D-2-385 / 2022

Cybernetica research reports are available online at
http://research.cyber.ee/

Mailing address:
Cybernetica AS
Mäealuse 2/1
12618 Tallinn
Estonia

EXECUTIVE SUMMARY

Cybernetica continues to develop its SplitKey SecureZone technology for threshold signing. An existing version of the technology has been Common Criteria certified. Recently, we have been looking for the most viable and value-added pathway to continued Common Criteria Evaluation for SplitKey SecureZone. In this document, we report our (public) findings, hoping them to be useful for other developers considering certification for their technologies. We have found that:

- It is not considered best practice to evaluate an existing version, and the evaluation process should coincide with the development of a future version of the Target of Evaluation (ToE).
- The publication of draft amendments to the existing eIDAS regulation on June 3rd, 2021, that suggest establishing a new EU eID Wallet and indicate that evaluating the current version has limited viability.
- Due to length of time for evaluation, if evaluation was to commence on the current version of Splitkey SecureZone its value may start declining after the adoption of the eIDAS regulation amendments and evaluation will not see a ROI.
- Planning a future release of SplitKey SecureZone around the amendments to the eIDAS regulations and beginning evaluation to coincide with development appears to be the most viable option.
- By starting the evaluation process, it is possible to list the next version of SplitKey SecureZone as ‘In Evaluation’.

Hence, we have made the following recommendations to Cybernetica. These should be transferable to other producers of similar technologies:

- Plan the next version of SplitKey SecureZone to develop in-line with the new protection profiles that emerge from the amendments to the eIDAS regulation and commence certification with that development cycle.
- For companies in the eID space engaging in common criteria evaluation projects, whose targets of evaluation might be affected by the changes to the eiDAS2 and / or integration into EU Wallet solutions, it is recommended to coincide the evaluation roadmap with their development roadmap, once more information around standards are published.

Index of Tables

Table of Contents

1 Introduction

1.1 Document Purpose

This document provides an overview of the proposed Common Criteria Evaluation process and business cases that may support it. Its recommendations and conclusions can help to shape the strategy for projects on certifying technologies similar to Cybernetica's SplitKey.

1.2 Background

Authentication and digital signing in European Union (EU) countries are regulated by the eIDAS regulation – regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, that came into effect on 1 July 2016. Even though eIDAS regulation is applicable only within the EU, a lot of third countries are implementing eIDAS voluntarily and eIDAS compliant and audited solutions are accepted as trustworthy solutions also outside the EU.

According to eIDAS regulation, electronic signing is a trust service. The electronic signature that is equal to the handwritten signature is called a qualified electronic signature. eIDAS regulation sets rules and requirements for such as service, including the requirements for certification and auditing. In order to be able to give qualified electronic signatures a trust service must be based on qualified electronic signature creation device (QSCD) – meaning a device that is certified as QSCD.

Cybernetica has a product called SplitKey which is a smartphone based secure authentication and electronic signing technology, based on threshold digital signatures. It can serve as the signature creation device (SCD) component in various trust services. In order for Cybernetica to be able to offer SplitKey to trust services, SplitKey needs to be QSCD certified according to eIDAS regulation. This certification would be done according to Common Criteria Certification, on EAL4+ level.

1.3 Strategic Objective

The objective of a common criteria evaluation project is to identify the most appropriate Target of Evaluation (ToE) to be certified. A technology provider, aiming for certification, has to choose, whether to apply for the certification of the current version of the technology, or some future version, developed in parallel to the common criteria evaluation project. Costs and opportunities of both options have to be studied, and compared against each other. The development of the EU wallet and changes to eIDAS have added further weight to certifying the future versions of the technology, as discussed further in this document.

1.4 EU Wallet and eIDAS

The European Commission proposed a framework on 3 June 2021, with amendments to the eIDAS regulation, including an EU Digital Identity that will be available to all EU citizens, residents, and businesses in the EU. The citizen wallet will be able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phones. They will be able to access online services with their national digital identification, which will be recognised throughout Europe. Very large platforms will be required to accept the use of European Digital Identity wallets upon request of the user, for example, to prove their age. The use of the European Digital Identity wallet will always be at the choice of the user.

To accelerate the path towards achieving this objective, Member States should increase their cooperation and identify a Toolbox for a European Digital Identity framework. The toolbox should lead to a technical architecture and reference framework, a set of common standards and technical references as well as best practices and guidelines as a basis for the implementation of the European Digital Identity framework. To ensure a harmonized approach for electronic identity in-line with the expectations of citizens and businesses, including of persons with disabilities, cooperation should start immediately in parallel and with full respect to the legislative process and alignment with its outcome.

This Recommendation sets up a structured process of cooperation between the Member States, the Commission, and, where relevant, private sector operators to develop the Toolbox. The Toolbox should cover four cross-cutting dimensions, namely the provision and exchange of identity attributes, functionality and security of the European Digital Identity Wallets, reliance on the European Digital Identity Wallet including identity matching, and governance. The Toolbox should meet the requirements laid out in the proposal for a European Digital Identity framework. It should be updated as necessary following the outcome of the legislative process.

Collaboration between the Member States is necessary for the exchange of best practices and the development of guidelines in areas where harmonisation is not required, but an alignment of practices would support the implementation of the European Digital Identity framework by Member State.

1.4.1 Process for developing a toolbox

Date	Proposal/Change
by September 2021;	Agreement on process and working procedures, the launch of data collection exercise from the Member States and discussion of technical architecture outline;
by December 2021;	Agreement on technical architecture outline;
by June 2022;	Identification of specific technical architecture, standards and references, guidelines, and best practices for: • The provision and exchange of identity attributes; • functionality and security of the European Digital Identity Wallets; • reliance on the European Digital Identity Wallets including identity matching; • governance;
by 30 September 2022;	Governance - the agreement between the Member States, in close cooperation with the Commission, on the Toolbox for the implementation of the European Digital Identity framework including a comprehensive technical architecture and reference framework, common standards, and technical references and guidelines and best practices;
by 30 October 2022;	Publication of the toolbox by the Commission.

Table 1-1- Development process for eIDAS2 toolbox

1.4.2 Content of the Toolbox

To facilitate the implementation of the European Digital Identity framework, it is recommended that the Member States cooperate to establish a toolbox including a comprehensive technical architecture and reference framework, a set of common standards and technical references, and a set of guidelines and descriptions of best practices. The scope of the toolbox should cover at least all aspects of the functionality of the European Digital Identity Wallets and of the qualified trust service for attestation of attributes as proposed by the Commission's proposal for a European Digital Identity framework. The content should evolve in parallel with and reflect the outcome of the discussion and process of adoption of the European Digital Identity Framework.

1.4.3 Common Standards and Technical References

It is recommended that Member States identify common standards and technical, references in particular in the following areas: European Digital Identity Wallets user functionalities including signing by means of qualified electronic signatures, interfaces and protocols, level of assurance, notification of relying parties and verification of their authenticity, electronic attestation of attributes, mechanisms for verifying validity of electronic attestations of attributes and associated person identification data, certification, publication of a list of European Digital Identity Wallets, communication of security breaches, verification of identity and attributes by qualified trust providers of electronic attestations of attributes, identity matching, minimum list of attributes from authentic sources such as addresses, age, gender, civil status, family composition, nationality, educational and professional qualifications, titles and licenses, other permits and payment data, catalogue of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes, cooperation, and governance.

1.4.4 Guidelines, best practices, and cooperation

It is recommended that the Member States identify guidelines and best practices in particular in the following areas: business models and fees structure, verification of attributes against authentic sources including via designated intermediaries. It is recommended that the Member States cooperate to update the deliverables resulting from this Recommendation after the adoption of the legislative proposal for a European Digital Identity Framework to account for the final text of the legislation.

1.5 Proposed Evaluation Options

Based on the aforementioned, there are two proposed pathways to certification with differing costs, timelines with considerations for changes to eIDAS regulation and new eID wallet road-maps have been announced that could possibly introduce an additional path for certifying involving different costs and should be considered as part of the 2nd option requiring further development. We see that a provider for a SplitKey-like technology has three main options for approaching its certification and development.

- **Option 1 -** Certify current version of the technology. This requires changes to documents created together with technology, but no new technical developments.
- **Option 2 -** Develop a new version of the technology, taking into account the developments in the legal landscape, and certify it.

1.6 Structure of this document

We are aiming this document towards both the decision-makers and engineers of an organization considering Common Criteria certification of their products. Hence, after introducing the key terminology in Sec. 2, we describe the different processes and their parts across the whole timeline in Sec. 3, and the different kinds of documentation used or created in these processes in Sec. 4. These two sections are aimed towards all stakeholders of the process, as is Sec. 5, where give some recommendations for successfully executing the evaluation process.

Sec. 6 is targeted towards engineers, giving an overview of assurance classes and families, which consist of assurance components that constitute a Security Target. This overview gives weight to our argument that certifying a piece of technology is itself a major undertaking. In Sec. 7, we discuss the components of the cost of performing a Common Criteria certification. This section is targeted more towards the decision-makers in the organization. Finally, Sec. 8 concludes this report.

2 Introduction to Common Criteria Evaluation

2.1 Common Criteria Overview

Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST), and may be taken from Protection Profiles (PPs) *(Higaki, pp31, 2010).* Vendors can then *implement* or make claims about the security attributes of their products, and testing laboratories can *evaluate* the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use. Common Criteria maintains a list of certified products, including operating systems, access control systems, databases, and key management systems.

2.2 Key Terminology

2.2.1 Target of Evaluation (ToE)

The Target of Evaluation is the product or subset of the product which is being evaluated. It is often not the entire product delivered to customers. When describing the ToE, it should be depicted in a block diagram of the system architecture with a dotted line around it. This high-level block diagram should include all major components whether they are part of the ToE or not. The ST document should describe in words each component. All security claims must be met by the ToE. *(Higaki, pp44, 2010)*

2.2.2 Protection Profile (PP)

A Protection Profile specifies generic security evaluation criteria to substantiate vendors' claims of a given family of information system products. PP’s can be standard by category or custom claims about the security of a product. The PP is the first item that requires mapping to a target of ToE to help determine requirements and assurances stated about the Security Target (ST) *(Higaki, pp58-59,146, 2010)*

2.2.3 Security Target (ST)

A Security Target defines security assurances and functional requirements for the given information system product, which is called the Target of Evaluation (TOE). An ST is a complete and rigorous description of a security problem in terms of TOE description, threats, assumptions, security objectives, security functional requirements (SFRs), security assurance requirements (SARs), and rationales. *(Higaki, pp141-143, 2010)*

2.2.4 Security Assurance Requirements (SAR)

Security Assurance Requirements (SARs) are descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the ST and PP, respectively. *(Higaki, pp141-143, 2010)*

2.2.5 Security Functional Requirements (SFR)

Security Functional Requirements are not requirements but claims and attributes of the ToE that will be evaluated. There is a standard set of claims that can be selected from CC part2 as well as the possibility of custom (explicitly stated SFRs) but it is recommended that instead of using custom SFRS it is better to request a modification to the standard. These are generally established in Phase 0 when creating a Protection Profile (PP). *(Higaki, pp151, 2010)*

2.2.6 Evaluation Assurance Level (EAL)

The Evaluation Assurance Level (EAL), a number 1 through 7, indicating the depth and rigour of the security evaluation, usually through supporting documentation and testing, that a product meets the security requirements specified in the PP. *(Higaki, pp61, 2010)*

2.2.7 Evaluated Environment

The evaluated environment is the IT and computing environment in which your product is deployed and operated. The ST document should describe the operational environment, computer hardware, operating system and network to be used in the evaluation. *(Higaki, pp46, 2010)*

N.B. *CC certificates are only valid for a single product version. Each certificate denotes the specific product version number. Efforts should be made to maximise the amount of time a products CC certificate is valid as re-certification can take 9-12 months. It is important to try to time the CC evaluations so as to minimise the time between product release and completing the evaluation.*

2.3 Roles & Responsibilities

Understanding the roles and responsibilities in the CC evaluation process is the first step in being able to determine resource allocation. The possible parties involved are *(Higaki, pp83, 2010)*;

- Developers, Engineering and QA team members.
- CC consultants / Technical writers
- CC evaluation lab
- Validators
- Executive Champion
- Project Manager

2.3.1 Developers, Engineering and QA

Developers, Engineering and QA are responsible as the product technical experts for explaining how the product was put together, how it was tested, and what features it has. The technical information provided by them is the core of the CC evaluation. *(Higaki, pp83, 2010)*

2.3.2 CC Consultants / Technical Writer

CC Consultants / Technical Writer are either third party or internal technical writers and are needed to augment or adapt existing technical documents for submission as evidence to the CC evaluators. It should be note that CC evaluators spend more time reviewing documents than actually testing products, thus the CC consultant role / Technical Writer is the therefore the most time consuming and important role. *(Higaki, pp84, 2010)*

2.3.3 CC Evaluation Lab

CC Evaluation Lab responsible for fulfilling the requirements described in the Common Evaluation Methodology (CEM). They will be responsible for evaluating evidence documentation, conducting any site visits, providing feedback and questions to the vendor and responding to comments from the scheme validators. *(Higaki, pp83, 2010)*

2.3.4 Validators

Validators are the national scheme government employees or contractors that who oversee the evaluation work of the evaluation lab. The scheme issues the official certificate to the vendor upon completion. Evaluators usually communicate with validators. *(Higaki, pp84-85, 2010)*

2.3.5 Executive Champion

Executive Champion or executive sponsor will help promote and defend the CC evaluation project. Even if a solid business case is presented to initiate the project, as time passes, business conditions may change and priorities shift. When that happens, it helps to have an executive sponsor who will defend the project. *(Higaki, pp85, 2010)*

2.3.6 Project Manager

Project Manager acts as the point of contact between the CC consultant, CC evaluation lab and development team. The adherence and adjustment of the schedule of the project is the responsibility of the project manager. *(Higaki, pp85, 2010)*

2.3.7 Business Analyst

Business Analyst is important role at the start of the project to help determine the overall business case supporting certification. Initial analysis should support the requirement for certification, the most appropriate type of certification and the cost / benefit analysis for determining ROI.

3 Process Overview

3.1 Phases of the Process Overview

The major phases required to complete a successful evaluation consist of 5 areas, each with their own deliverables, key performance indicators and major milestones *(Higaki, pp43, 2010).* Major milestones also act as phase gates in the regards that these milestones must be met and noted before moving onto the next phase. Work on a subsequent phase cannot often not commence without achieving the major milestone. *Stratton, R. W. (2003)*

Phase Number	**Phase Stage**
Phase 0	Pre-Evaluation Preparation
Phase 1	Project Launch
Phase 2	Evaluation & Feedback
Phase 3	Validation & Certification
Phase 4	Assurance Maintenance

Table 3-1 - Evaluation phase numbers and stages

The following subsections describe the phases. They start with the list of key deliverables and milestones of the phase, as well as performance indicators associated with them. The subsections continue with the description of the most important aspects of each phase.

3.2 Phase 0: Pre-Evaluation Preparation

Key Deliverable	Key Performance Indicators	Major Milestone
Business Case Research Paper	Acceptance of Business Case	
Project Scope Statement Project Charter Project Management Plan	Approval of Project Document Pack	

Protection Profile (PP) Mapping to (ToE)	Agreement on SFR mapping to ToE	
	Agreement on SAR mapping to EAL	
	Acceptance of Partner Selection	Agreement with Evaluation Partner

Table 3-2 - Phase 0 Deliverables, KPI's and Major Milestone

3.2.1 Researching Certification Requirements

This research may not be entirely applicable for internal certification projects, but is still recommended as part of forming a coherent business case. *(Higaki, pp58, 2010)*

If certification is also required to satisfy specific customer requirements or reflect potential customer expectations, the following questions may need to be answered;

- Is the evaluation be performed against a particular Protection Profile (PP)?
- Is there a specific Evaluation Assurance Level (EAL) requirement?
- What are the required Security Functional Requirements (SFR) to be included in the evaluation?
- What product version is going to be evaluated?
- Why does the product need to be CC evaluated?
- What other (competitors) products have already been evaluated?
- On what platforms (Evaluation Environment) will the evaluation be performed and certified for.

3.2.2 Protection Profile Requirements

A Protection Profile is basically a set of CC requirements for a particular product type. It contains Security Functional Requirements (SFR) and Security Assurance Requirements (SAR) which typically maps to an Evaluation Assurance Level (EAL). Some product types map directly to a Protection Profile (PP), whilst other products, including threshold signing solutions, require additional custom requirements not standardised in existing PP's. The PP is the cornerstone of developing the Security Target (ST) document and needs to be identified early in the Phase 0 cycle. *(Higaki, pp58-60, 2010)*

Current Standard Common Criteria PP's can be found at:

https://www.commoncriteriaportal.org/pps/

N.B. *There appears to be a new PP in development from the BSI which maps directly to cryptography services which can be viewed here*.

3.2.3 Evaluation Assurance Level (EAL) Requirement

When evaluating against a Protection Profile, the PP dictates the EAL, against which the ToE must be evaluated. The EALs are a standard set of Security Assurance Requirements (SARs)that determine the breadth and depth the evaluators will check and examine the evidence. EAL 1 to EAL7 is the current range. An example target is EAL4+ *(Higaki, pp61-62, 2010)*

3.2.4 Understanding the Common Criteria Standards

Before commencing the evaluation process, it is recommended to have an understanding of the standards of which the CC process is held to, insights and advice from those who are directly experienced with CC. The process can be long and expensive if inexperienced and knowing how to best navigate it will reduce cost and time. *(Higaki, pp67, 2010)*

Common Criteria standards are developed for flexibility as it was the intention to use them to evaluate the security of a variety of IT products. The Common Criteria Portal (CC Portal) is the website for information pertaining to the CC standards. It contains standards documents and also supporting documents (SD). The website also has links to national schemes related to CC. *(Higaki, pp69, 2010)*

The Common Criteria Users Forum (CCUF) also has resources and a helpful FAQ section that explains CC simply for vendors. *(Higaki, pp70, 2010)*

The International Common Criteria Conference (ICCC) is another resource for understanding and interacting with evaluators, certification bodies, policy makers etc and other professionals involved with the CC. *(Higaki, pp70, 2010)*

3.2.5 Pre-Evaluation Questions, Processes & Product Knowledge

As part of the pre-evaluation preparation, it is wise to ask the development team for the following documents so how much work can be estimated based on the existence and accuracy of existing documentation. Example documents that should be requested are *(Higaki, pp71, 2010)*;

- Product User Manuals
- Product Architecture Diagram and Descriptions
- User-visible error messages
- Test Packages
- Product Delivery Processes
- Defect Management Processes
- Source Code Control tools and Processes
- Documentation used previously in CC for re-use

If embarking on a new certification project the following topics should be discussed with the development team to ascertain the current state of readiness and to gauge how much preparation work is required. *(Higaki, pp72-73, 2010)*

- Configuration Management
- Delivery and Operation
- Design and Architecture
- Guidance Documentation
- Testing
- Vulnerability Analysis
- Product Features

3.2.6 Developing a compelling Business Case – Costs

There are two main components to developing a ROI business case to pursue a CC evaluation; Costs and Benefits. Understanding how much the CC evaluation will cost relies on understanding requirements. The major cost categories are *(Higaki, pp75-77, 2010),*

- CC consultant or in-house evidence development costs
- Evaluation Lab Costs
- Travel expenses for consultants and evaluation lab personnel
- Validators fees (if applicable from the national scheme)
- Equipment costs for any special test set-ups

Lost opportunity costs need to also be factored in. Baseline estimations indicate to allow for 500 person hours for EAL4 and 250 person hours for EAL2 just for the development team. Though this is a general figure that may reflect an IAR process or re-certification of an existing product where documentation can be re-used. These figures are dependent on the complexity of the PP and ToE and may increase if some existing documents need to be changed or new documents created. *(Higaki, pp78, 2010)*

The general costs calculation at a high-level overview for estimation should follow this formula *(Higaki, pp79, 2010)*;

Total Costs = Evaluation Lab Costs + CC Consultant Costs + Other Expenses + Validators Fees + Equipment Costs + Lost Opportunity Costs

An example cost for EAL4+ certification is $500,000 USD

3.2.7 Developing a Compelling Business Case – Benefits

To complete the ROI analysis, you will need to understand and quantify the benefits of CC Evaluation. One of the main motivators for CC evaluation can be losing competitive advantage to a rival company. Typical approaches to quantifying the benefits include *(Higaki, pp79-82, 2010)*;

- CC Evaluation status of competitors products.
- Historical data on deals lost to competitors with CC evaluated products.
- Incremental revenues of upcoming contracts that require CC evaluations.
- Timing of CC evaluations
- Competing or similar evaluations
- ROI scenarios of not proceeding or delaying evaluation.

3.2.8 Allocating Resources

It is critical that proper resource allocation is performed to ensure the competition of the evaluation project. Resource allocation and requirements vary greatly if existing documentation is to the standard required, if a CC consultant is engaged and the experience of staff with evaluations. If resources cannot be effectively planned and allocated, an evaluation project is destined to fail. *(Higaki, pp82, 2010)*

Time is spent in the following 5 categories *(Higaki, pp86, 2010)*;

- Assembling the raw technical information
- Formatting documentation for the CC evaluators
- Developing special test cases
- Responding to CC evaluators questions.
- Updating documentation from previous certification efforts

It is recommended to have a CC consultant onboard for first time certifications as this will seriously reduce the amount of rework required for a successful evaluation. The most significant delays experienced by other vendors is where internal documentation is lacking and the authors were no longer with the company. *(Higaki, pp87, 2010)*

Developers / QA can expect to be required 20 person hours per week in the pre-evaluation stage phase 0. Reducing to 2 person hours per week in evaluation phase 2. Project managers can expect a minimum of 3 person hours per week once the project has kicked off. Internal Technical Writers can expect full use of their time during the project if it is to be conducted in a timely fashion. This is why many companies use the services of an outside CC consultant to generate the documentation for the CC evaluation lab. *(Higaki, pp89, 2010)*

3.2.9 Managing Project Scope

As CC evaluations can be sizeable projects, they can be prone to time and therefore cost overruns. Recommendations regarding best practices for project scope management are *(Higaki, pp94-94, 2010)*;

1. Meet minimum requirements
2. Minimise changes to the plan
3. Leverage existing evidence

Meeting minimum requirements is focused on reducing the scope of the evaluation to be a specific as possible with a very narrow ToE. This will reduce greatly documentation requirements, testing etc. Suggested minimisation strategies include *(Higaki, pp94-95, 2010)*;

- Assess customer minimum requirements
- Avoid Protection Profiles that aren't suitable
- Minimise the ToE scope
- Minimise complexity of system configurations
- Minimise ST / EAL claims
- Avoid misusing CC evaluations

3.2.10 Selecting Partners

There are many CC evaluation and CC consulting partners available to work with, aside from the usual cost, technical expertise, terms and co-operation factors, early engagement is by far the most important consideration. This will assist in the accurate creation of the ST document and the development of an Evaluation Work Plan (EWP) for planning purposes. *(Higaki, pp109-127, 2010)*

3.3 Phase 1: Project Launch

Key Deliverable	Key Performance Indicators	Major Milestone
Security Target (ST) Document	Acceptance of the Security Target (ST) document	
Project Management Plan mapped to EWP	Agreement on the Evaluation Work Plan (EWP)	
	Approval of the Project Management Plan	Kick-off Meeting with the 'Scheme' agenda

Table 3-3 - Phase 1 Deliverables, KPI's and Major Milestone

3.3.1 Launch Overview

The launch phase centres around the generation of the Security target (ST) document, submitting the ST document and acceptance of the CC evaluation by the evaluator. It also includes all the activities to prepare for the kick-off meeting such as agreement on the Evaluation Work Plan (EWP). *(Higaki, pp43-44, 2010)*

3.3.2 Security Target Document Overview

Security Target (ST) document frames the Common Criteria (CC) evaluation effort. It answers the question – What is being evaluated? It is the foundation on which all the rest of the CC evidence documentation is built and drives all evaluation activities. The ST document must include *(Higaki, pp44, 2010)*;

1. Target of Evaluation (ToE)
2. Evaluated Environment
3. Evaluation Level (EAL4+)

Additionally, the ST document must *(Higaki, pp141-144, 2010)*:

- Claim compliance with an applicable approved Protection Profile.
- Contain a clear and complete description of the ToE physical and logical boundaries.

- Contain a clear definition of components both within and outside of the TOE

3.3.3 ST Document Format

The ST definition and scope describes what will be evaluated and to what depth. All other documents are to be consistent with the ST document. The ST document maybe produced internally or with the assistance of a CC consultant. Depending on the experience of internal staff and nature of the ST, hiring a CC consultant to write the ST document, may speed up the creation of this document. The format of the ST document is as follows *(Higaki, pp141-143, 2010);*

- Introduction
  - ST Reference
  - ToE Reference
  - ToE Overview
  - ToE Description
- Conformance Claims
  - CC Version
  - PP Conformance Claims
- Security Problem Definition
  - Threats
  - Organisational Security Policies
  - Assumptions
- Security Objectives
  - ToE Security Objectives
  - Environmental Security Objectives
  - Security Objectives Rationale
- Extended Components Definition
- Security Requirements
  - Security Functional Requirements
  - Security Assurance Requirements

    - Security Requirements Rationale
- ToE Summary Specification
    - Security Functions
    - ToE Security Specifications

3.3.4 Evaluation Work Plan (EWP)

The evaluation work plan is a plan developed by the CC evaluation lab, developer and CC consultant. It outlines who will deliver what by when. This is an initial plan that will likely change and be adjusted throughout the CC evaluation project. *(Higaki, pp47-48, 2010)* An example EWP is given below. It is structured by the CC Assurance Classes and Families, described in Sec. 6 giving a deadline, where the claims supporting each assurance family will have been fully documented and delivered to the CC evaluation lab.

CC Assurance Class	CC Assurance Family	Target Delivery Date
Security Target (ASE)		13th August 2020
Configuration Management (ACM)	Capability (CAP) Configuration Identification and CM System evidence	27th September 2020
Delivery and Operation (ADO)	Delivery (DEL)	27th September 2020
	Installation, Generation & Start-up (IGS)	27th September 2020
Life Cycle Support (ALC)	Flaw Remediation (FLR)	27th September 2020
Guidance Documents (AGD)	Administrator (ADM)	5 October 2020
	User (USR)	5 October 2020
Development (ADV)	Functional Specification (FSP)	9 November 2020
	High-Level design (HLD)	9 November 2020
	Representation Correspondence (RCR)	9 November 2020

Tests (ATE)	Test Coverage (COV)	9 November 2020
	Developer tests (FUN)	9 November 2020
Vulnerability Assessment (AVA)	Strength of Function (SOF)	20th February 2021
	Vulnerability Analysis (VLA)	20th February 2021
	Misuse Potential (MSU)	20th February 2021

Table 3-4 - Example Evaluation Plan

N.B: *The dates used above are indicative only and are intended to provide an example of an evaluation plan, not the proposed plan itself.*

3.3.5 Kick-off Meeting with the 'scheme' agenda

The kick-off meeting is largely a formality as the preparation should have addressed any issues. It is the first major milestone of the CC evaluation. *(Higaki, pp48-49, 2010)*

- Purpose of the meeting
- Introduction of participants
- Identify roles and responsibilities of the various parties
- Identify key point points of contact
- Review the organisation and goals
- Sponsor / Vendor introduces the product (ToE)
- Review sponsor / vendor schedules
- Review Evaluation plans and schedule
- Review expectations and goals
- Plan future meetings
- Address questions or concerns
- Acceptance into 'in evaluation'

N.B. *To support sales, at this stage it is ideal for the technology vendor to request the evaluation lab and Scheme body update their website list of products in evaluation to reflect that the vendor has been accepted into evaluation. (Higaki, pp49-50, 2010)*

3.4 Phase 2: Evaluation and Feedback

Key Deliverable	Key Performance Indicators	Major Milestone
Security target (ASE) Evidence Document/s	Approval of ASE	
Configuration Management (ACM) Evidence Document/s	Approval of ACM	
Delivery and Operation (ADO) Evidence Document/s	Approval of ADO	
Guidance Documents (AGD) Evidence Document/s	Approval of AGD	
Life cycle Support (ALC) Evidence Document/s	Approval of ALC	
Development (ADV) Evidence Document/s	Approval of ADV	
Tests (ATE) Evidence Document/s	Approval of ATE	
Vulnerability Assessment (AVA) Evidence Document/s	Approval of AVA	
		Final Evaluation Test Report (ETR) submitted

Table 3-5 - Phase 2 Deliverables, KPI's and Milestones

3.4.1 Evaluation Overview

The evaluation and feedback phase are a series of cycles of evidence production, evaluation, comment, modification, re-submission and re-evaluation iterated until the evaluator is satisfied. *(Higaki, pp50-53, 2010).*

3.4.2 Evaluation Process

Tasks performed on each evidence document deliverable-based

- Evidence production by the CC consultant with input from the development team
- Evaluation by the CC evaluation lab personnel
- Comments on the evidence by the CC evaluation lab sent back to the vendor (Cybernetica)
- Modification of the evidence to address comments
- Re-submission of the evidence
- Re-evaluation by the CC evaluation lab

3.4.3 Work Units

- Security target (ASE)
- Configuration Management (ACM)
- Delivery and Operation (ADO)
- Guidance Documents (AGD)
- Life cycle Support (ALC)
- Development (ADV)
- Tests (ATE)
- Vulnerability Assessment (AVA)

***N.B**. The work units are elaborated on in depth in chapter 6 of this document.*

3.4.4 Documentation Considerations

Each work unit involves the evaluation of one or more evidence documents that are intended to support the vendor claims in the Security target (ST) document. Evidence documentation builds upon each other to provide support of the arguments the Target of Evaluation (ToE) meets the security claims.

Example. *The ST will claim that the ToE supports a security function such as data protection. The functional specification document (part of development) must describe the data protection functions. The internal design documents must support and be consistent with the functional specifications of the data protection features. The test plans must illustrate how the data protection features were tested.*

3.4.5 Site Visit – needs to be a direct quote or paraphrased

For most evaluations the CC evaluator will visit the vendor’s development site to observe at least the use of the configuration management system. Often this visit will also be used to check testing and delivery procedures. This site visit will require dedicated time from the development team and QA staff. Most site visits take 2-5 days. If the development team are distributed across sites several sites, the CC evaluator may want to visit those other sites to make sure that the procedures at each site meet the EAL stated requirements. *(Higaki, pp53, 2010)*

3.4.6 Evaluation Timeline

The Evaluation Timeline can take 7-18 months. However, if the same technology has been previously certified, perhaps in a certain context, then the timeframe may be significantly shorter, due to the proposed requirements of only having to make minor documentation changes on the previous submission and engage in site visits as per 3.4.5 There is the possibility that the technology vendor may be able to perform the certification process by submitting an IAR as per the Phase 4 process, described in Sec. 3.6.

3.5 Phase 3: Validation and Certification

Key Deliverable	Key Performance Indicator	Major Milestone
Common Criteria Evaluation Report	Acceptance of the final ETR	Common Criteria Certification Issued

Table 3-6 - Phase 3 Deliverables, KPI's and Milestone

3.5.1 Validation Overview

In the validation phase the ETR is received by the validators of the scheme from the CC evaluation lab and the validators review the results. They may ask questions of the evaluation lab and conclude the evaluation was successful. If there are issues noted by the validators, they must be resolved before the certification can be issued. *(Higaki, pp53, 2010)*

3.5.2 Validation Process

Once the final ETR from the evaluator is sent to the Scheme, the Scheme will then complete their final review. Once the review and any issues are resolved, the CC certification is issued. *(Higaki, pp53, 2010)*

3.5.3 Validation Timeline

The validation and certification phase typically takes 2 weeks to 2 months. *(Higaki, pp53, 2010)*

3.5.4 Validation Outcome

The ST, final certification report and a copy of the CC certificate are usually posted on the Scheme's website. *(Higaki, pp53, 2010)*

3.6 Phase 4: Assurance Maintenance

Key Deliverable	Key Performance Indicator (KPI):	Major Milestone
Impact Analysis Report (IAR)	Acceptance of the IAR without complete re-evaluation	Version or incremental update of ToE

Table 3-7- Phase 4 Deliverable, KPI and Milestone

3.6.1 Assurance Maintenance Overview

As CC certificates are only valid for a single version of a product and the re-certification process can take between 6-18 months, the Assurance Maintenance mechanism exists to shorten the re-evaluation cycle. *(Higaki, pp54, 2010)*

3.6.2 Assurance Maintenance Process

The assurance Maintenance process requires documenting changes to the ToE and supporting that security has not been compromised by supply evidence outlined in the IAR document. *(Higaki, pp54, 2010)*

3.6.3 Assurance Maintenance Outcome

The desired outcome of submitting an IAR mapped to an incremental or version update is to not have to restart the certification process entirely thus reducing time and cost overheads in the re-certification process. *(Higaki, pp54, 2010)*

3.6.4 Assurance Maintenance Timeline

The Assurance Maintenance timeline is unclear and dependant on the number of changes and evidence required to support any claims that security has not being compromised. By having a thorough IAR prepared it may save much more time. *(Higaki, pp54, 2010)*

4 Documentation Development

4.1 List of required evidence

Evidence documents serve to support the claims made about the ToE. There are numerous documents required, which may already partially exist in various forms. The complete list of evidence which may be required are *(Higaki, pp131, 2010)*;

- Security Target (ST)
- Security Architecture
- Functional Specifications
- ToE Design
- Implementation representation
- Preparation procedures
- Configuration management (CM) capabilities
- CM Scope
- Delivery
- Development security
- Flaw remediation
- Life cycle definition
- Tools and techniques
- Test coverage
- Test depth
- Functional tests
- Independent tests
- Vulnerability assessment

4.2 5 factors rating system

For each evidence type an assessment should be made against 5 factors and each factor given a rating level of *low (1), medium (2) or high (3).* These ratings should reflect the current circumstances regarding evidence documentation. The 5 factors are *(Higaki, pp132, 2010)*;

- Acceptable materials exist to serve as CC documentation
- Developer would learn more about their production
- CC knowledge is needed to develop the CC documentation
- Detailed developer input is needed to develop the CC document
- Internal resources availability

4.3 Evidence Creation Collaboration

Recommendations for what evidence documents should be done by the developer and what evidence documents should be a collaboration between developers, evaluators and consultants are as follows *(Higaki, pp132-133, 2010)*;

Developer created evidence:

- Operational user guidance
- Preparation procedures
- Configuration Management (CM) capabilities
- CM scope
- Delivery
- Development security
- Flaw remediation
- Life cycle definition
- Tools and techniques
- Test coverage
- Test depth
- Functional Tests

Jointly developed evidence:

- Security Architecture
- Functional specifications
- ToE design
- Implementation representation
- Independent tests

4.4 Evidence development tips

The two most common approaches to organising document development are Organising by evaluation activity and organisation by documentation set. Organisation by evaluation activity breaks down the documentation work into the standard evaluation categories; ST, development, guidance, life cycle, test and vulnerability assessment. Organisation by documentation set follows the categories of documentation i.e., Architecture, ToE (Higaki, pp134-135, 2010).

Tips for consideration regarding evidence development are;

- Identify subject matter technical experts early and keep them available.
- Be diligent about delivery of evidence to maintain the schedules.
- Allow time for unexpected events that may delay the schedule.

4.5 Using CC Consultants

The role of CC consultants varies greatly form turn key solutions to just advising on a specific document. The services they offer are generally *(Higaki, pp134-136, 2010)*.;

- Advice
- Review
- Templates, examples or questionnaires
- Evidence creation
- Provide complete, turnkey solutions

Some considerations when engaging CC consultants are;

- Who owns the evidence once it has been created?
- Consultants may have the same level of understanding of the CC but have different perspectives
- Better consultants will yield better results
- Providing too much information may open areas of evaluation that are not security relevant
- Providing too little information may result in the rejection of evidence by the evaluator or more questions.

4.6 Common issues in document development

There are commonly referenced issues in the CC evaluation process that can impact the document development process. These common issues can be minimised if managed correctly from the start of the project and some CC consultants have automated tools to assist in mitigating them *(Higaki, pp137-140, 2010)*.

- Invalid references in documents
- Problems with the SFR specifications
- SFR Conflicts
- Conflicts between overview and description
- Mappings and rationale
- Learning curve for internal staff in CC evaluations
- Introducing methodology changes
- Overload of paperwork and document review
- Lost opportunity costs

5 Successful CC Evaluation Recommendations

5.1 Best Practices

The key best practices can be summarised as *(Higaki, pp179, 2010)*:

- Meet minimum requirements
- Allocate time
- Minimise changes to the plan
- Reuse certification materials
- Weekly status calls with evaluators
- Dedicated technical writer
- Synchronise evaluation with development.

5.1.1 Meet Minimum Requirements

Minimise the Security Functional Requirements (SFRs) claims and the EAL for their evaluation. Consider any organisational level changes that may affect the evaluation processes. Consider external changes and competitor behaviours against the same PP and EAL *(Higaki, pp180-181, 2010)*.

5.1.2 Allocate Time

Experience will best dictate how long an evaluation will take to complete. As more evaluations occur, team members will become more comfortable with estimating their time. Project managers and team members need to work together to allocate their time to evaluation so that is meshes with their other activities. This global resource allocation approach will help deliver the evaluation in a timely fashion and minimise the impact on other development projects *(Higaki, pp181-182, 2010)*.

5.1.3 Minimise Changes to the Plan

Changes to the product will force re-evaluation of some of the evidence that has already been evaluated. In a business environment where change is rapid and constant, the CC evaluation project team is challenged to stay on course. Any changes to versions being evaluated should be done prior to the evaluation process begins as changes will create waste in lost time and increase costs. Likewise waiting for the next version to commence evaluation must be a known factor when weighing up which version to evaluate *(Higaki, pp182-183, 2010)*.

5.1.4 Reuse Certification Materials

Initial document creation is very resource heavy, however once a successful evaluation has taken place, certain documents can be reused with little or minor modifications. If there are common procedures across different business units in a company, this can also enable faster and less costly successful evaluations *(Higaki, pp183-184, 2010)*.

5.1.5 Weekly Status Calls with Evaluators

Hold weekly status calls with the evaluators that that include all stakeholders; program manager, development lead, lead engineer, CC consultant or technical writer, the evaluators etc. it is important to get everyone into reporting statuses on a weekly basis. This also helps to establish an effective working relationship with the evaluators *(Higaki, pp184, 2010)*.

5.1.6 Dedicated Technical Writer

Equally important as the commitment of the development and QA teams to evaluation is the assignment of a dedicated technical writer. The responsibility of this writer is to transform raw technical details from the development and QA teams into CC evidence documentation that the evaluators can easily consume. This technical writer can be contracted, a CC consultant or a member of the company / technical writing staff *(Higaki, pp185, 2010)*.

5.1.7 Synchronise Evaluation with Development

Evaluation should be synchronised with the product development process. An evaluation can be too early or too late in the product development cycle. Time between product release and validations should be minimised. Ideally you would co-ordinate the development of the CC evidence documentation with the product development phase that would naturally generate the necessary technical content *(Higaki, pp185-187, 2010)*.

i.e., Security Architecture and design evidence should be procured during the product design phase.

CC evaluations are only valid for the specific version of the product, and whilst engaging a CC evaluation can start too early it is also possible for a CC evaluation to start too late.

N.B. *Expert advice is to try and avoid starting a CC evaluation on a product version that is already shipping to customers – aim to evaluate a future version.*

5.2 Project Management Fundamentals

The CC evaluation is a challenging project. It involves co-ordinating third parties and internal teams. The pressure to perform is heightened by its cost and length. It is recommended that a Project manager is assigned and responsible for *(Higaki, pp187, 2010)*:

- Planning – establish the overall evaluation project plan and make real-time adjustments as needed throughout the process.
- Monitoring – continuously monitor progress and identify issues that affect the plan.
- Controlling – mitigate issues and update the plan as necessary.

5.2.1 Planning

In the planning phase the Project Manager should liaise closely with team members to establish everyone time required and when they are required. This process itself can contribute to help to identify requirements to minimise scope and establish the ToE boundary *(Higaki, pp187-188, 2010)*.

5.2.2 Monitoring

During weekly status calls review the progress toward the current set of deliverables, discuss any issues that may delay any deliveries and develop contingency plans. Also look ahead at the next set of deliverables and make sure any dependencies are being addressed *(Higaki, pp188-189, 2010)*.

5.2.3 Controlling

The successful CC evaluation project manager must drive the product team's responsiveness to inquiries from the evaluation lab. Delays in responding can hinder the success of the project *(Higaki, pp189-190, 2010)*.

5.3 Managing Customer Expectations

Whatever the stated customer requirements are, it is important to get them to articulate the requirements as clearly and precisely as possible. Getting details from the customer helps focus the evaluation, reduces cost and saves time. If customers state they require evaluation to be success for a tender, ask them what type of evaluation certification and what level of evaluation. i.e., EAL4+ *(Higaki, pp190-191, 2010)*.

Once evaluation is underway it is advantageous to communicate this to customers or potential customers.

6 Overview of Assurance Families

This chapter gives an enumeration of the assurance families of the CC and the various assurance classes introduced and described in Part 3 of the CC. BSI (pp10-12, 2007) give a somewhat longer overview of these classes and families.

Assurance Class	Assurance Family	Name and Description
Development	ADV_ARC	**Security Architecture** The security architecture family provides requirements for a security architecture description that describes the self-protection, domain separation, non-bypass principles, including a description of how these principles are supported by the parts of the TOE that are used for TSF initialisation.
	ADV_FSP	**Functional specification** This family contains requirements upon the description of the TSF interfaces (TSFI). The TSFI consist of all means for users to invoke a service from the TSF (by supplying data that is processed by the TSF) and the corresponding responses to those service invocations.
	ADV_IMP	**Implementation representation** The function of this family is for the developer to make available the implementation representation of the TOE in a form that can be analysed by the evaluator. The implementation representation is expected to be in a form

		that captures the detailed internal workings of the TSF.
	ADV_INT	**TSF Internals** This family addresses the assessment of the internal structure of the TSF. A TSF whose internals are well-structured is easier to implement and less likely to contain flaws that could lead to vulnerabilities; it is also easier to maintain without the introduction of flaws.
	ADV_SPM	**Security policy modelling** There are no requirements of this family for EAL1 to EAL5.
	ADV_TDS	**TOE design** The requirements of the TOE design family are intended to provide information so that a determination can be made that the security functional requirements are realised. The goal of design documentation is to provide sufficient information to determine the TSF boundary, and to describe how the TSF implements the Security Functional Requirements.
Guidance Documents	AGD_OPE	**Operational user guidance** Requirements for operational user guidance help ensure that all types of users are able to operate the TOE in a secure manner. It should be excluded that the TOE can be used in a manner that is insecure but that the user of the TOE would reasonably believe to be secure
	AGD_PRE	**Preparative procedures** Preparation requires that the delivered copy of the TOE is accepted, configured and activated by the user to exhibit the protection properties as needed during operation of the TOE.
Lifecycle Support	ALC_CMC	**CM capabilities** Configuration management capabilities define the characteristics of the configuration management system.
	ALC_CMS	**CM scope** Deals with the scope of the CM system which indicates the TOE items that need to be controlled by the CM system. This is reflected by the required contents of the configuration list to be provided.
	ALC_DEL	**Delivery** The concern of this family is the secure transfer of the finished TOE from the development environment into the responsibility of the user.
	ALC_DVS	**Development security** Development security covers the physical, procedural, personnel, and other security measures used in the development environment. It includes physical security of the development location(s) and controls on the selection and hiring of development staff.
	ALC_FLR	**Flaw remediation**

		Flaw remediation ensures that flaws discovered by the TOE consumers will be tracked and corrected while the TOE is supported by the developer.
	ALC_LCD	**Life-cycle definition** Life-cycle definition establishes that the engineering practises used by a developer to produce the TOE include the considerations and activities identified in the development process and operational support requirements. Confidence in the correspondence between the requirements and the TOE is greater when security analysis and the production of evidence are done on a regular basis as an integral part of the development process and operational support activities.
	ALC_TAT	**Tools and techniques** Tools and techniques are an aspect of selecting tools that are used to develop, analyse and implement the TOE. It includes requirements to prevent ill-defined, inconsistent or incorrect development tools from being used to develop the TOE. This includes, but is not limited to, programming languages, documentation, implementation standards, and other parts of the TOE such as supporting runtime libraries.
Security Target Evaluation	ASE_CCL	Specific to the PP
	ASE_ECD	
	ASE_INT	
	ASE_OBJ	
	ASE_REQ	
	ASE_SPD	
	ASE_TSS	
Tests	ATE_COV	**Coverage** This family assures that the TSF has been tested against its functional specification. This is achieved through an examination of developer evidence of correspondence.
	ATE_DPT	**Depth** The components in this family deal with the level of detail to which the TSF is tested by the developer.
	ATE_FUN	**Functional tests** Functional testing performed by the developer provides assurance that the tests in the test documentation are performed and documented correctly. The correspondence of these tests to the design descriptions of the TSF is achieved through the Coverage (ATE_COV) and Depth (ATE_DPT) families.
	ATE_IND	**Independent testing** This family deals with the degree to which there is

		independent functional testing of the TSF.
Vulnerability Assessment	AVA_VAN	**Vulnerability analysis** This class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE. It is an assessment to determine whether potential vulnerabilities identified during the evaluation of the development and anticipated operation of the TOE or by other methods

Table 6-1 - Assurance family class, units & descriptions (BSI, 2007)

7 Cost analysis

7.1 Cost Definitions

The recommended formula for use in a CC evaluation and the definitions of each item are listed in the subsequent sections.

7.1.1 Formula

To calculate the general cost at a high level, the following formula is used:

Total Costs = Evaluation Lab Costs + CC Consultant Costs + Other Expenses + Validators Fees + Equipment Costs + Personnel cost*+ Lost Opportunity Costs *(Higaki, pp79, 2010)*

7.1.2 Evaluation / Auditors Lab Costs

Current evaluation lab or auditors cost estimates are general estimates that can only be determined from a full quotation after an evaluation partner is selected, as are their travel and accommodation costs. To determine the exact cost currently requires a pathway to be selected. The cost of the Evaluation Lab should not vary across the different pathways, unless there is multiple Targets of Evaluation (ToE) *(Higaki, pp75-82, 2010)*.

7.1.3 CC Consultants Cost

CC Consultants / Technical Writer are either third party or internal technical writers and are needed to augment or adapt existing technical documents for submission as evidence to the CC evaluators *(Higaki, pp75-82, 2010*.

7.1.4 Other Expenses

These additional costs stipulated as ‘other costs’ are consistent across each option. It is anticipated, these costs should not exceed 10,000 EUR and are almost exclusively related to the travel, transportation, incidentals and accommodation expenses of the evaluators site visit

(Higaki, pp75-82, 2010).

7.1.5 Validator's Fees

Validators are the national scheme government employees or contractors that who oversee the evaluation work of the evaluation lab. Their fees are typically part of the evaluation labs costs and are currently considered to be included, however in some circumstances additional costs may be added by validators. If any validators cost is included in the evaluation cost, and if the vendor is based in a country without a relevant national validation scheme, then these costs will most likely be through BSI/ANSSI *(Higaki, pp75-82, 2010)*.

7.1.6 Equipment Costs

This cost pertains to physical equipment for the evaluation environment such as servers, switches and other infrastructure required to demonstrate the operating environment of the ToE. *(Higaki, pp75-82, 2010).* There is an existing equipment cost associated with certifying the Cloud HSM component of a SplitKey-like technology. The equipment costs of future versions may be difficult to estimate due to the changing standards, which should be taken into consideration.

7.1.7 Personnel cost

Personnel costs, other than staff costs, could be considered as a "*lost opportunity costs*" in many cases.

7.2 Cost Analysis Summary

Across the 2 potential options for the pathway to certification, there are potential hidden costs that are currently not able to be estimated. This is mainly to do with the lost opportunity costs.

The evaluation lab certification is based on the previous estimates, but is subject to change based on the pathway chosen forward. A more comprehensive quotation can be obtained once the option is chosen and added to the final cost analysis in the internal research document deliverable.

8 Summary

Evaluating an existing version of software is not considered best practice due to the length of time for certification. By the time certification is completed, typically after 18 months, the next version of software is beginning its development phase. Adding weight to the position that better value can be derived from evaluating a future version of the software implementing the technology, external factors arising from the government and scheme announcements regarding standards to adhere to. This creates a possible dead-end for the versions of software that do not have a good match with the upcoming changes in the industry.

This however presents companies with an opportunity to leverage off the changes in the marketplace to develop their next version of software solutions that is compliant with the emerging standards and other integrations (if applicable) and design their development lifecycles around these changes for maximum value of a successful evaluation.

By commencing this development phase to coincide with these outside factors and the commencement of the evaluation of the next version of their software solution, companies can create the optimal value and effective resource planning for the evaluation project, due to time window for development and maximising the lifetime of the evaluation.

Recommendation:

For companies in the eID space engaging in common criteria evaluation projects, whose targets of evaluation might be affected by the changes to the eiDAS2 and / or integration into EU Wallet solutions, it is recommended to coincide the evaluation roadmap with their development roadmap, once more information around standards are published.

9 References

Higaki, W.H.: Successful Common Criteria Evaluation. A Practical Guide for Vendors. Wesley Hisao Higaki, Lexington (2010)

Stratton, R. W. (2003). Project gates: "Chutes and Ladders®" for project managers. Paper presented at PMI® Global Congress 2003—EMEA, The Hague, South Holland, The Netherlands. Newtown Square, PA: Project Management Institute.

BSI. Guidelines for Developer Documentation according to Common Criteria, version 3.1 (2007)