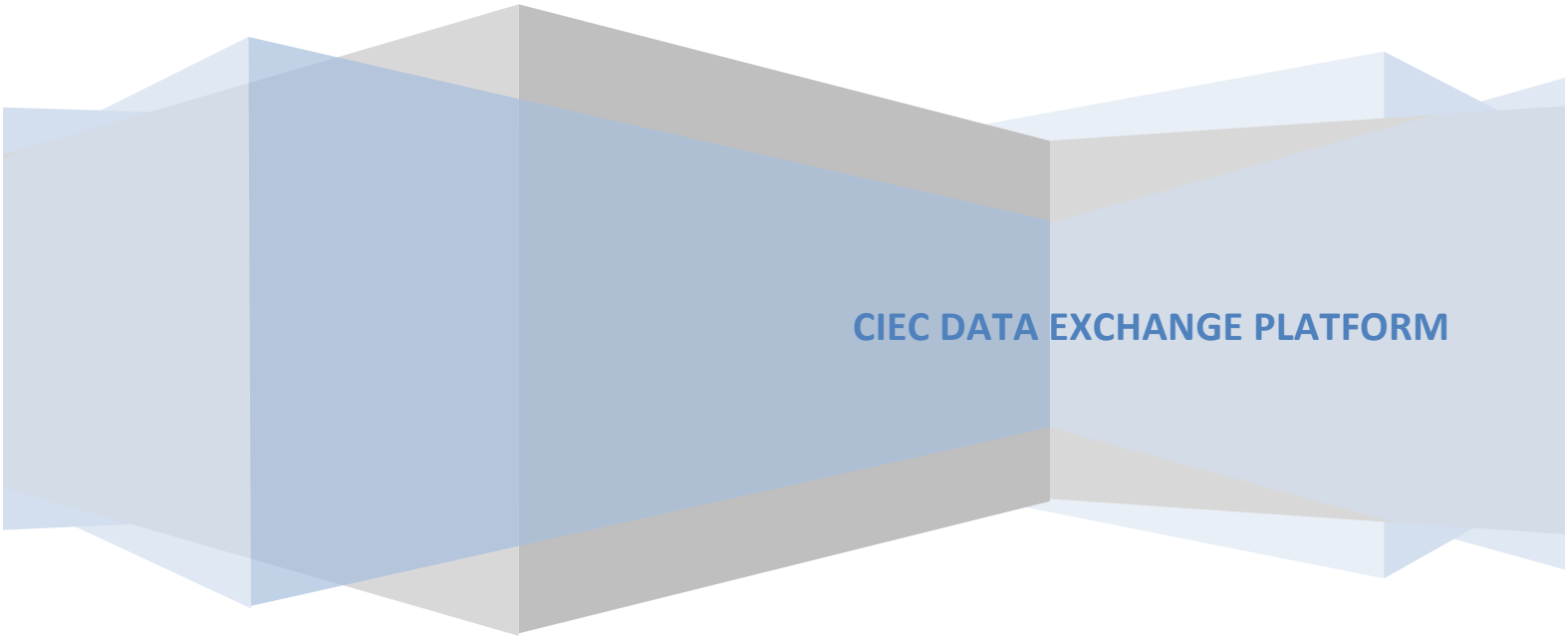
UBITECH
ubiquitous solutions

ICCS-CIEC

Requirements and Effects of CDEP on End-user Workstations

Draft Version



CIEC DATA EXCHANGE PLATFORM

27 February 2012

Index

List of Tables

Notational conventions

This document uses the following conventions:

- Terms in bold are used to indicate definitions. These may include subsystems (**Authority Maintenance**), entities (**Task**), business processes (**Document Exchange Procedure**) and any other notion related to the *ICCS-CIEC Data Exchange Platform*.
- Terms in italics are used to indicate:
  - Subsystems, e.g. *Authority Maintenance*.
  - Entities, e.g. *Task.*
  - System actors, e.g. *Owner*.
  - Service operations, e.g. *initiate Task*
- Numbers in square brackets with the "Ref" prefix are used to represent references, e.g. [Ref12]. Clicking on them will forward the reader to the actual reference in the document's appendices.
- Each reference to an ICCS-CIEC Data Exchange Platform or any external artefact is accompanied by its acronym in brackets when it first occurs. Thereafter, only the acronym is used.

Abbreviations

For the purposes of the present document, the following abbreviations apply:

Abbreviation	Term
API	Application Programming Interface
CDEP	CIEC Data Exchange Platform
CA	Certification Authority
HSM	Hardware Security Module
JKS	Java Key Store
JRE	Java Runtime Environment
JCE	Java Cryptography Extension
JWS	Java Web Start
OS	Operating System
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
SEP	Signing & Encryption Program

Table 1 : Abbreviations

Introduction

This document was compiled following the 4th meeting of the CIEC IT Experts, which took place in Paris on 9-10 February 2012. It serves a twofold purpose: to present the prerequisites of the *CIEC Data Exchange Platform (CDEP)* client-side programmes, and to describe the effects of their operation on end users' workstations.

The CDEP's end-user functionality is achieved by a combination of web-based and desktop programmes working in synergy. The client applications are web-based and, thus, they are served by web browsers and require no extra software. The CDEP's desktop clients are standalone *Java Web Start (JWS)* programmes. They run on the client workstation's *Operating System (OS)*. They require some software artefacts, such as libraries and configuration files. Most dependencies are satisfied by the bootstrap programme and, therefore, they are not presented here. The current document describes only the core dependencies, requiring manual intervention. Besides software, there is some hardware that the CDEP's client applications require, in order to operate properly. This will be also described in detail.

It should be noted that this document makes no mention of any software or hardware prerequisites relating to security, which includes *Hardware Security Modules (HSMs)* (USB dongles, smart cards, etc.), as well as the corresponding software drivers and management programmes. Each CDEP end-user workstation already has a security system in place, which varies according to country or regional specifications and, therefore, it is assumed that the appropriate software has been successfully installed and configured.

As well as detailing the CDEP's requirements, this document describes the effects of running CIEC applications, focusing on the files to be added to each workstation's hard drive. Special care has been taken, in order to minimize the space occupied by these files on the end user's hard drive, and to operate strictly on user-space, with no need for any special OS privileges.

Finally, it is important to emphasise that the set of requirements and effects described in this document refer to the current status of CDEP. This may change in future versions. Among other criteria, we are concentrating our efforts on minimizing both requirements and effects in order to create a system that is not intrusive with regard to end users' workstations.

Dependencies

Software

[Dep1] Web Browser. Currently, only Chrome and Firefox have been fully tested with CDEP web applications. They are shortly to be tested with other browsers, as shown in the following table :

Browsers	Support Level
Google Chrome 7+	OK
Firefox 3+	OK
Internet Explorer 8+	Under testing
Opera 10+	Under testing
Safari	Under testing

Table 2 Browsers & level of support

[Dep2] *Java Runtime Environment (JRE)* v1.6.*xx*. CDEP has been tested only in a Java 6 environment. Using any other version of JRE, whether prior or subsequent to version 6, is strongly discouraged. If JRE is not present, then the bootstrap program will attempt to download and install the latest JRE subversion of version 6. However, this solution is strongly discouraged, since it requires administration privileges and may disrupt the stability of any existing software.

[Dep3] *Java Cryptography Extension (JCE)* Unlimited Strength Jurisdiction Policy Files 6 ([Ref1]). The JCE architecture allows the flexible configuration of cryptographic strength according to jurisdiction policy files. Due to some countries' import restrictions, the jurisdiction policy files distributed with JDK 6 software have built-in restrictions on available cryptographic strength. The jurisdiction policy files in the referenced download bundle do not restrict cryptographic strength. Since CDEP is required to meet high security standards, the installation of this bundle is mandatory. The installation procedure is described in the README file included in the bundle. In order to install this bundle to a client's workstation OS, administration privileges are required.

[Dep4] Write access to the user's home directory. Since the bootstrap programme installs files in a directory within the user's home directory, it is assumed that it will be granted write access to this directory.

We assume that the bootstrap programme will, logically, have read access to the pre-installed *PKCS#11* ([Ref4]) libraries, used for signing purposes, since workstation users already use it.

Hardware

CDEP JWS programmes have no special requirements in terms of hardware; if plain JRE 6 requirements are fulfilled, this should suffice ([Ref3]). However, for ease of use, the following minimum requirements should be fulfilled:

Attribute	Minimum Value
Main memory	1 GB
CPU	1 GHz
HDD	256 MBs free
Internet access	Broadband
Screen resolution	1280x720

Table 3 Minimum requirements for good quality user experience

Effects of usage

The CDEP has minimal effects on the end user's workstation. The only effect will be that files will be added to the hard drive. More specifically:

[Eff1] A new directory will be created [<*user_home_dir*>/**.ciecKI**/], containing the following files:

- **myks:** *Java Key Store (JKS)* , containing the office credentials plus the server certificate.
- **myks.p12:** *PKCS#12* version of myks ([Ref5]).
- <***PKCS#11 driver library***>: the driver programme library of the *PKCS#11* compatible device, which accesses qualified credentials used for signing purposes. If there is a library reference (e.g. C:\Windows\System32\pkcs11.dll) in the local OS installation, no library will be installed in this directory.
- **sgn.cfg**: *PKCS#11* signing configuration text file.
- **signKS:** Directory including the set of signing configuration types (binary, non-executable files), named **out<*xxx*>**, where *xxx* is an incremental integer.

[Eff2] Java Web Start will install a cache directory, named *.java* or *.javaws* or *javaws*, under a subfolder, or directly under the user home directory. This local cache will host the CDEP application jars in digest form (there will be no jar files that can be directly accessed and used).

References

[Ref1] Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6, http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html

[Ref2] CIEC Security Analysis Document, https://www.ciec-platform.org/CIECEnvironment/Security_Aanlysis_Document_WP4_Final_20_01_2012-sig.pdf

[Ref3] System requirements for Java 6, http://www.java.com/en/download/help/sysreq.xml

[Ref4] PKCS #11: Cryptographic Token Interface Standard, http://www.rsa.com/rsalabs/node.asp?id=2133

[Ref5] PKCS #12: Personal Information Exchange Syntax Standard, http://www.rsa.com/rsalabs/node.asp?id=2138