PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/46

ZoneCentral v3.1 build 533

Paris, 18th of December 2008

Courtesy Translation

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.

Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

Certification Report reference **DCSSI-2008/46**
Product name **ZoneCentral**
Product reference/version **Version 3.1 build 533**
Conformity with a protection profile **none**
Evaluation criteria and version **Common Criteria version 2.3** **compliant with ISO 15408:2005**
Evaluation level **EAL 2 augmented** **ADV_HLD.2, ADV_LLD.1*, ADV_IMP.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1*, AVA_MSU.1, AVA_VLA.2** ***applied to FCS requirements**
Developer(s) **Prim'X Technologies** **10 Place Charles Béraudier, 69428 Lyon Cedex 03, France**
Sponsor **Prim'X Technologies** **10 Place Charles Béraudier, 69428 Lyon Cedex 03, France**
Evaluation facility **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France** **Phone: +33 (0)1 30 14 19 00, e-mail : cesti@oppida.fr**
Recognition arrangements **CCRA** **SOG-IS**

Introduction

Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr

Table of contents

1. The product

1.1. Presentation of the product

The evaluated product is “ZoneCentral, Version 3.1, build 533” developed by Prim’X Technologies.

This product is used in ensuring the confidentiality of files processed by users on isolated workstations, laptop computers, or on workstations connected to a corporate network. It makes it possible to encrypt the files, without changing their characteristics (location, name, date, size). This encryption is carried out as transparently as possible for the users: in fact, the files are encrypted “in-place” (where the files are located, thus without changing the user’s data structure) and “on the fly” (at the request of the user, without any specific manipulation other than the entering of the key access codes required for the decryption).

1.2. Description of the product

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operating environment.

1.2.1. Product identification

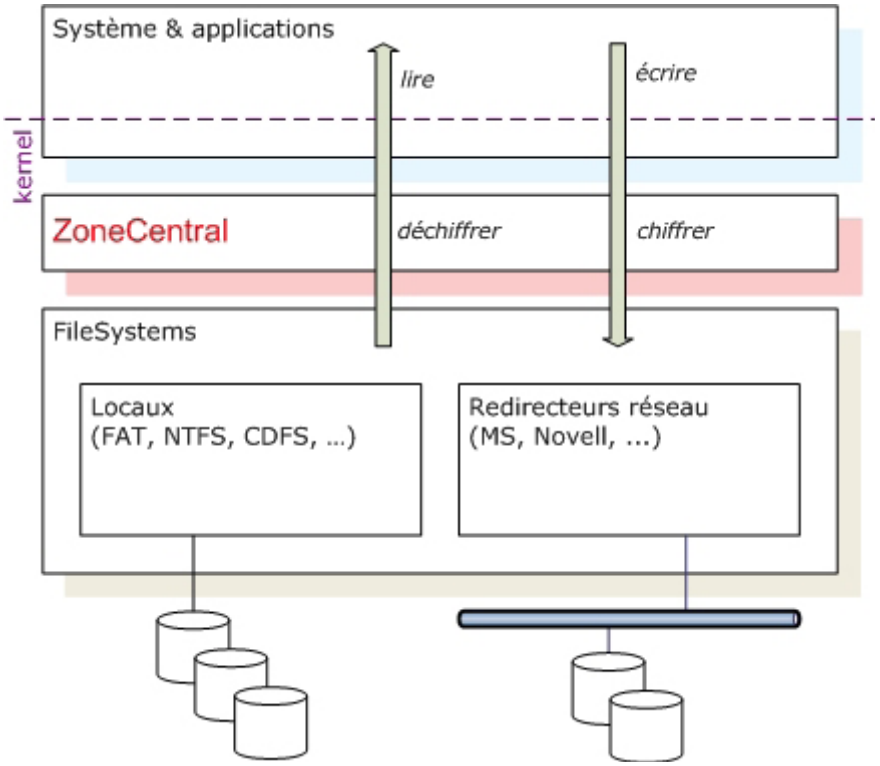
The component elements of the product are identified in the configuration list [CONF].
The certified version of the product is identifiable by the “About” window which gives the product version as well as its build number (in this case version 3.1, build 533).
The integrity of the product can be checked by a comparison of the Authenticode signatures generated by the user or the administrator with those available on the developer’s web site.

1.2.2. Security services

The TOE provides the following services:
- Administration of the product in command mode and in graphic mode;
- Definition of encrypted zones;
- Management of access rights for the encrypted zones;
- Coordination of processing between the “user” world and the “kernel” world;
- Filtering of access to the files;
- Cryptographic operations for managing the zone keys and the associated calculations;
- Windows Winlogon extension (Login screen for opening a session);
- Windows Explorer extension for the personalisation of the encrypted file icons;
- Auditing of events linked with the operations performed by the product.

1.2.3. Architecture

Under Windows, a file belongs to a file management system (NTFS, FAT, CDFS, etc.) which stores and manages it. All the file management systems provide access methods for the files they host, in a relatively homogeneous and universal form, and in such a way that the applications accessing the files do not normally have to take account of the nature of the file management system hosting their files.
Any application, any system component under Windows that accesses a file (open a file, read part of its contents, write, rewrite, add data, etc.) submits its requests to a mechanism that allocates these to the relevant file management system for the file in question.
ZoneCentral integrates with the Windows kernel and positions itself in the file management system strings, applying a filter technology positioned for this purpose in these strings. Positioned in this way, it receives (and then retransmits to the next element in the string) all requests submitted for all of the files of all the file management systems it filters. During the forwarding of these requests, it can carry out certain operations as required: decrypting the read portion when this involves the reading of an encrypted file, or alternatively encrypting the written portion when this involves writing to an encrypted file, or again perform a complete data wipe when a file has been deleted.



This product acts as a security layer integrated in the system; it is transparent for the users and enables the security policy to be applied for all file systems: local, fixed, network, etc.

The following elements are included in the evaluation perimeter:
- the PKCS#11 dialogue between the TOE and the user tokens;
- the PKCS#12 dialogue between the TOE and key files;
- the network dialogue between the TOE and the user data stored on remote media (for instance, a server on a local network or on the Internet).

The following elements are outside the evaluation perimeter:
- The keyboard dialogue between the TOE and the inputting of the passwords;
- The Windows operating systems, including:
    - The PC/SC drivers;
    - The certificate management service (CMS);
    - The user profile management service (User management);
- The tokens used (such as USB Token type tokens, key files or CSP containers);
- The sorting of user access keys (RSA keys in the tokens or passwords supplied by the product administrator).

1.2.4. Lifecycle

The lifecycle of the product is as follows:
- The development and delivery of the product on the PRIM'X site in Lyon;
- The installation, administration and use of the product corresponding with the deployment of the product by the customer.

For a single workstation use of this product, the [GUIDE_USR] guide describes all the product's functionalities that can be implemented by a user who is also an administrator of the workstation.
For its use in a company, where the administration and user roles are generally separated, the [GUIDE_ADM] guide describes the administration functionalities of the product corresponding with a centralised management of the applicable security policies for the workstations on which the product has been installed. The [GUIDE_USR] guide describes the functionalities available to the user. The extent of rights possessed by the users depends on the configuration chosen by the administrator.

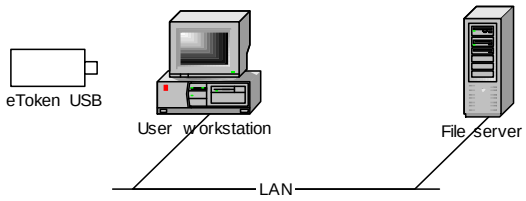
The product was developed on the following site:

Prim'X Technologies

10 Place Charles Béraudier
69428 Lyon Cedex 03
France

1.2.5. Evaluated configuration

The test platform implemented by the CESTI corresponds with the following configuration:



This test platform used virtualised operating systems. This choice does not have any implications for the evaluation of this product. The product integrates with the Windows kernel and positions itself in the file management system strings (ZoneCentral acts as a logic

filter between the operating system and the file system offered by the host machine), and the virtualisation technology acts upstream of these processes.
The tokens that were used on this platform were Aladdin brand eToken 72K pro, the Windows certificates store and a PKCS#12 key container.

The certificate thus covers the following operating environment:
- Operating systems: Microsoft Windows 2000, Windows XP, Windows Vista and Windows 2003;
- Interfaces with zone access key supports: PKCS#11 and PKCS#12.

2. The Evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM].

2.2. Evaluation work

The technical evaluation report [RTE], submitted to the DCSSI on 15 December 2008 provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has been analysed by DCSSI. The results obtained are stated in the cryptographic analysis report [ANA-CRY].
The analysed mechanisms reached the standard level as defined in DCSSI cryptographic referential (Cf. [REF-CRY]), under condition of the application of the recommendations contained in the guides [GUIDES].

3. The certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product "ZoneCentral, Version 3.1, build 533" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 2 augmented.

3.2. Restrictions

This certificate covers the product as specified in section 1.2 of this Certification Report.

The user of the certified product shall respect the environmental security objectives as specified in the security target [ST] and follow the recommendations contained in the guides [GUIDES] supplied, notably:

- The users and/or administrators must check the integrity of the product (OE.SOFT_SIGNE);
- The installation of the product must be carried out in accordance with its installation manual (OE.INSTALLATION);
- The physical environment for the use of the product must enable the users and administrators to enter their passwords without these being directly observable or without it being possible for this process to be intercepted by other users or potential hackers; organisational arrangements must make it possible for the administrator to authenticate a remote user prior to any forwarding of a backup password (OE.NON_OBSERV);
- When the user has been authenticated, the operational environment must ensure the confidentiality of sensitive data and of the authentication data (OE.ENV_OPERATIONNEL);
- The users and the administrators of the product must be trustworthy (OE.SO_CONF, OE.ADM_ROOT_WINDOWS);
- Users and administrators must prevent the disclosure of the access keys for the encrypted zones (OE.CONSERV_CLES);
- Users and administrators must be aware of the issue of data security and be trained in using the product (OE.FORMATION, OE.ADM_DELEGATION);
- Users and administrators must be aware of the issues of the quality of the access keys as well as that of their support (OE.CRYPTO_EXT);
- Users and/or administrators must check the validity of the X509 certificates and their suitability for the use that is made of these by the product; this requirement applies in particular to the "authenticode" root certificates used for checking the integrity of the product (OE.CERTIFICATS);
- The administrators of the Windows domain must prohibit sublevel administrators from modifying the security policies of the product (OE.ADM_ROOT_WINDOWS).

3.3. Recognition of the Certificate

3.3.1. European Recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

3.3.2. Common Criteria Recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, Norway, Netherlands, Spain, Sweden and United Kingdom.

2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom and United States.

Appendix 1. Evaluation level of the product

Class	Family	Components by level of assurance							Level of assurance chosen for the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 2+	Component
ACM Configuration Management	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**2**	Configuration items
	ACM_SCP			**1**	**2**	**3**	3	3		
ADO Delivery and Operation	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1***	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1***	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guidance	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Life-cycle Support	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3	**1***	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**1**	Evidence coverage
	ATE_DPT			**1**	1	**2**	2	**3**		
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing – sample
AVA Vulnerability assessment	AVA_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

** applied to FCS requirements*

Appendix 2. Evaluated product references

[ST]	Reference security target for the evaluation: - « ZoneCentral version 3.1 - Cible de Sécurité CC niveau EAL2+ », reference CSZC31, version 2, revision 6
[RTE]	Evaluation technical report : - « Rapport technique d'évaluation – Projet ZEBRA2 », ref. OPPIDA/CESTI/ZEBRA2/RTE, version 1.0
[ANA-CRY]	« Cotation de mécanismes cryptographiques – Projet ZEBRA2 », N°1436/SGDN/DCSSI/SDS/Crypto, 3 July 2008
[CONF]	« Liste de configuration de la version 3.1 Build 533 », réf. PX81112, version 1, revision 3
[GUIDES]	[GUIDE_ADM] Product installation and administration guide: - "ZoneCentral - Administrator technical manual - Version 3.1", Reference: PX81098, revision 5 [GUIDE_USR] Product User's Guide: "ZoneCentral, Version 3.1 – User Guide", Reference: PX81092, revision 3

Appendix 3. Certification references

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. The content of Common Criteria version 2.3 is identical to that of the International ISO/IEC 15408:2005 Standard.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of Common Criteria version 2.3 is identical to that of the International ISO/IEC 18045:2005 Standard.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Cryptographic mechanisms – Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level, current version, see: www.ssi.gouv.fr