Reference: 2017-3-INF-2526-v1
Target: Público
Date: 11.10.2018

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-3**
TOE	**FusionAccess Software version V100R006C20**
Applicant	**440301192W - HUAWEI Technologies Co., Ltd.**

References

[EXT-3261] Certification Request

[EXT-4304] Evaluation Technical Report

Certification report of the product FusionAccess Software version V100R006C20, as requested in [EXT-3261] dated 17/01/2017, and evaluated by Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-4304] received on 28/09/2018.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product FusionAccess Software version V100R006C20.

This is a virtualization product that centralises and delivers virtual desktops and applications to end users. End users can access their virtual desktops and applications wherever connection is available. The TOE provides a web portal graphical user interface (GUI) for administrators to quickly provision, maintain, and reclaim virtual desktops and applications. This helps to elastically manage virtual resources, improve resource utilization, and reduce operational expenditure (OPEX).

Developer/manufacturer: HUAWEI Technologies Co., Ltd.

Sponsor: HUAWEI Technologies Co., Ltd.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Epoche & Espri S.L.U.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R4 EAL3 + ALC_FLR.2

Evaluation end date: 28/09/2018.

All the assurance components required by the evaluation level EAL3 (augmented with ALC_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 + ALC_FLR.2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product FusionAccess Software version V100R006C20, a positive resolution is proposed.

TOE SUMMARY

The TOE provides the following key security features:

- Identification and Authentication: Only authenticated local administrators can access management portal to provision, maintain, and reclaim virtual desktops and applications. If authentication is failed, local administrator cannot access the TOE. Only authenticated end users can access AccessClient application and WI web portal to gain access to virtual desktops and published applications assigned by a local administrator. In case of multiple authentication failure in a row the affected account is locked to avoid unauthorized access.

- Security Audit: An operation log records the operations that a local administrator has performed on the system and the result of the operation and is used for tracing and auditing. Only local administrator can review and query the records. Operation logs are stored in such a way that unauthorized modifications are prevented.
- User access policy: local administrator can assign virtual desktops and applications to end users. End users only can access to their permitted virtual desktops and applications. Local administrator can set end user access policy to determine whether the end users can access to local device resources such as USB device, the clipboard or local drivers.
- Secure communications: TOE server can be accessed by TLS creating a trusted path between the TOE and the end user.
- Security management: local administrator is able to configure the password policy, the user attributes, set lock timeouts, lock/unlock accounts, end user access control policy, and local resource policy. The TOE is able to manage different user roles.
- TOE Access: The TOE is able to manage the concurrent multiple sessions by limiting the number of active sessions per user. The TOE is also able to terminate an interactive session after an inactivity period of time.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 R4.

Class	**Family/Component**
ADV Development	ADV_ARC.1, ADV_FSP.3, ADV_TDS.2
AGD Guidance Documents	AGD_OPE.1, AGD_PRE.1
ALC Life-Cycle Support	ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, **ALC_FLR.2**
ASE Security Target evaluation	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
ATE Tests	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA Vulnerability Assessment	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Common Criteria v3.1 R4:

Class	Component
FAU: Security Audit	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FAU_STG.1 FAU_STG.3
FDP: User Data Protection	FDP_ACC.1 FDP_ACF.1
FIA: Identification and Authentication	FIA_AFL.1 FIA_SOS.1 FIA_UID.2/end user FIA_UID.2/local administrator FIA_UAU.2/end user FIA_UAU.2/local administrator
FMT: Security Management	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1
FPT: Protection of the Security Functions	FTP_TRP.1
FTA: TOE Access	FTA_MCS.1 FTA_SSL.3

IDENTIFICATION

Product: FusionAccess Software version V100R006C20

Security Target: Huawei FusionAccess V100R006C20 Security Target, Version 1.4, 2018-09-27 [ST].

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R4 EAL3 + ALC_FLR.2.

SECURITY POLICIES

The use of the product FusionAccess Software version V100R006C20 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the [ST], chapter 3.5 (Organizational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.4 (Assumptions) are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.3 (Threats) do not suppose a risk for the product FusionAccess Software version V100R006C20, although the agents implementing attacks have the attack potential according to the Basic attack potential of EAL3 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

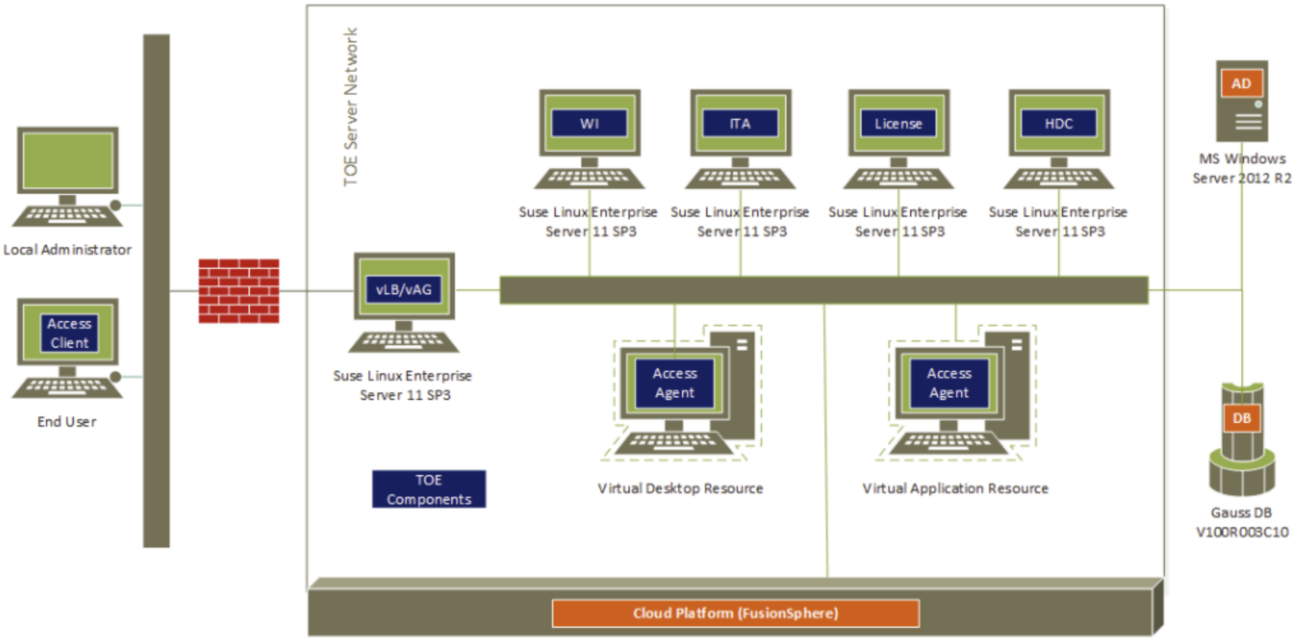
The security objectives declared for the TOE operational environment are detailed in [ST], chapter 4.2 (Security Objectives for the Operational Environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target [ST].

ARCHITECTURE

LOGICAL ARCHITECTURE

The following figure provides an architectural overview of the product FusionAccess Software version V100R006C20, the elements displayed with a blue background are components of the TOE.


TOE Server Network
Local Administrator
Access Client
End User
WI
ITA
License
HDC
Suse Linux Enterprise Server 11 SP3
Suse Linux Enterprise Server 11 SP3
Suse Linux Enterprise Server 11 SP3
Suse Linux Enterprise Server 11 SP3
AD
MS Windows Server 2012 R2
vLB/vAG
Suse Linux Enterprise Server 11 SP3
Access Agent
Access Agent
DB
TOE Components
Virtual Desktop Resource
Virtual Application Resource
Gauss DB V100R003C10
Cloud Platform (FusionSphere)

The TOE is composed by following components:

Component	Function Description
ITA	The ITA provides interfaces for administrator to manage desktops and application. It interacts with the HDC and FusionSphere to create and assign VMs, manage VM status and images, and operate and maintain VMs.

HDC	As the core of the virtual desktop management software, the HDC manages desktop groups, assigns VMs to users, un-assign VMs from users, and enables users to log in to VMs after receiving requests from the ITA.
License	The license component manages and distributes licenses for the HDC and restricts the amount of users who login virtual desktop.
WI	The WI provides a web login page for end users. After an end user initiates a login request, the WI forwards the user login information (the encrypted username and password) to the AD for authentication. If the authentication succeeds, the WI displays a desktop and application list provided by the HDC to the user. The user can choose a desktop or application from the list to log in.
vLB/vAG	The vLB implements load balancing of WIs to prevent a large number of users from accessing the same WI (in case of there are more than one instance for each TOE component). The vAG serves as the access gateway to connect to the elements located at the internal network.
AccessClient	AccessClient installed on user devices and enabled HDP connections from user devices to virtual desktops and published applications.
AccessAgent	AccessAgent software installed on VMs and enables VMs to interact with desktop management components

PHYSICAL ARCHITECTURE

The physical boundary of the TOE is integrated by the TOE Server and TOE Client components.

The TOE Server components consist of ITA, WI, HDC, License, vLB/vAG and AccessAgent (which is installed in the managed VMs). The TOE Client component is the AccessClient running on a user device.

The TOE software packages are binary compressed files. The following software packages and documents are required:

Type	**Name**	**Version**	**Delivery Format**

Software	FusionAccess	V100R006C20	.iso file
Software	FusionAccess Client	V100R006C20	.msi file
Software	FusionAccess Tools	V100R006C20	.iso file
Document	[AGD_PRE] CC Huawei FusionAccess V100R006C20 Preparative procedures	0.7	.docx format
Document	[AGD_OPE] CC Huawei FusionAccess V100R006C20 Operational user guidance	0.8	.docx format

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

Type	Name	Version	Delivery Format
Document	[AGD_PRE] CC Huawei FusionAccess V100R006C20 Preparative procedures	0.7	.docx format
Document	[AGD_OPE] CC Huawei FusionAccess V100R006C20 Operational user guidance	0.8	.docx format

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the evaluator premises.

In addition, the laboratory has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and, in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product FusionAccess Software version V100R006C20 it is necessary the disposition of the following components:

- Hardware platform[1] in which the virtual servers can be installed.
- Huawei FusionSphere that virtualizes hardware resources so that one physical server can function as multiple virtual machine:
  - Item: v100R006C00U1_FusionSphereInstaller.zip
  - Item: FusionCompute V100R006C00U1_VRM.zip
  - Item: FusionCompute V100R006C00U1_CNA.iso
- The TOE components and non-TOE components which are virtualized inside the cloud platform, which are:
  - WI/ITA/HDC/License server and vLB/vAG server with SUSE Linux Enterprise Server11 SP3
  - The WI/ITA/HDC/License server has a Database with Huawei GaussDBV100R003C10
  - AccessAgent for virtual desktop with Microsoft Windows Windows Server 2012 R2 Standard and Microsoft .NET framework with version 1.6.20005.10694 (V100R006C20).
  - A Domain controller with a Microsoft Active Directory Domain Service of Windows Server 2012 R2 Standard.
- A PC with Windows 7 32-bits operating system where CloudClient application is installed:
  - CloudClient application with version 1.6.20005.0 (V100R006C20).
- A PC with Debian 9 placed between external network and internal network acting as a firewall, with the configuration specified in the document [AGD_PRE].

[1] The evaluated platform has been FusionServer H22H-03 (RH2288H V3).

EVALUATION RESULTS

The product FusionAccess Software version V100R006C20 has been evaluated against the Security Target [ST].

All the assurance components required by the evaluation level EAL3 + ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL3 + ALC_FLR.2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The TOE usage is recommended as there are not exploitable vulnerabilities for the TOE under its operational environment.

The following usage recommendations are given:

- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.
- The user guidance must be read and understood in order to operate the TOE in and adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Epoche & Espri S.L.U., a positive resolution is proposed.

The certifier strongly recommends potential consumers to follow specific security instructions provided in preparative [AGD_PRE] and operational guidance [AGD_OPE] as well as to observe the assumptions provided in the Security Target [ST].

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target of Evaluation
VM	Virtual Machine

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[AGD_OPE] FusionAccess V100R006C20. Operational User Guidance. Version 0.8, 2018-08-28

[AGD_PRE] FusionAccess V100R006C20. Preparative Procedures. Version 0.7, 2018-08-27

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.

[ST] Huawei FusionAccess V100R006C20 Security Target, Version 1.4, 2018-09-27

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Huawei FusionAccess V100R006C20 Security Target, Version 1.4, 2018-09-27.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.