



DL02321LAB/000

Membro degli Accordi di Mutuo Riconoscimento EA, IAF e ILAC
Signatory of EA, IAF and ILAC Mutual Recognition Agreements

Certificato di Accreditamento

Accreditation Certificate

Accreditamento n.
Accreditation n. **02321 Testing REV. 00**Emesso da
Issued by **Dipartimento Laboratori di Prova**Si dichiara che
We declare that **ATSEC Information Security srl**
Sede/Headquarters:
- Via Santa Croce in Gerusalemme 63 - 00185 Roma RME' conforme ai requisiti
della norma **UNI CEI EN ISO/IEC 17025:2018**Meets the requirements
of the standard **ISO/IEC 17025:2017**Quale **Laboratorio di Prova**As **Testing Laboratory**Data di 1^a emissione
1st issue date
22-10-2025Data di revisione
Review date
22-10-2025Data di scadenza
Expiring date
21-10-2029

L'accreditamento attesta la competenza tecnica, l'imparzialità e il costante e coerente funzionamento del Laboratorio relativamente al campo di accreditamento riportato nell'Elenco Prove allegato al presente certificato di accreditamento.

Il presente certificato non è da ritenersi valido se non accompagnato dagli Elenchi Prove, che possono variare nel tempo e può essere sospeso o revocato o ridotto in qualsiasi momento nel caso di inadempienza accertata da parte di ACCREDIA.

La validità dell'accreditamento può essere verificata sul sito web (www.accredia.it) o richiesta al Dipartimento di competenza.

I requisiti di sistema della ISO/IEC 17025 sono scritti in un linguaggio attinente alle attività di laboratorio e sono generalmente in accordo con i principi della norma ISO 9001 (si veda comunicato congiunto ISO-ILAC-IAF dell'Aprile 2017).

The accreditation attests competence, impartiality and consistent operation in performing laboratory activities, limited to the scope detailed in the attached Enclosure.

The present certificate is valid only if associated to the annexed Lists and can be suspended, withdrawn or reduced at any time in the event of non fulfilment as ascertained by ACCREDIA.

Confirmation of the validity of accreditation can be verified on the website (www.accredia.it) or by contacting the relevant Department.

The management system requirements in ISO/IEC 17025 are written in language relevant to laboratories operations and generally operate in accordance with the principles of ISO 9001 (refer joint ISO-ILAC-IAF Communiqué dated April 2017).

Il QRcode consente di accedere direttamente al sito www.accredia.it per verificare la validità del certificato di accreditamento rilasciato al CAB.

La data di revisione riportata sul certificato corrisponde alla data di aggiornamento / di delibera del pertinente Comitato Settoriale di Accreditamento. L'atto di delibera, firmato dal Presidente di ACCREDIA, è scaricabile dal sito www.accredia.it, sezione 'Documenti'.

The QRcode links directly to the website www.accredia.it to check the validity of the accreditation certificate issued to the CAB.

The revision date shown on the certificate refers to the update / resolution date of the Sector Accreditation Committee. The Resolution, signed by the President of ACCREDIA, can be downloaded from the website www.accredia.it, 'Documents' section.

ACCREDIA è l'Ente Unico nazionale di accreditamento designato dal governo italiano, in applicazione del Regolamento Europeo 765/2008.

ACCREDIA is the sole national Accreditation Body, appointed by the Italian government in compliance with the application of REGULATION (EC) No 765/2008.

ATSEC Information Security srl Via Santa Croce in Gerusalemme 63 00185 Roma RM	UNI CEI EN ISO/IEC 17025:2018
	Revisione: 0 Data: 22/10/2025
	Sede A pag. 1 di 2

ELENCO Prove Accreditate - Con Campo Fisso in Categoria: 0

Applicative security/, Communication protocols/, Cryptographic Mechanisms/, Databases/, Embedded systems, microkernels/, Filtering/, Hardware components protocols/, Intrusion detection/, Low-level interfaces/, Network protocols/, Personal computer and server security/, Phone and VoIP/, State-of-the-art of Approved Cryptographic Mechanisms/, Virtualization/, Web technologies/, Wireless/, Mobile networks/

Denominazione della prova / Campi di prova	Metodo di prova	Tecnica di prova	O&I
IT Common Criteria security evaluation up to AVA_VAN.2 - Cryptographic analysis/ : Conformity analysis and tests/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + ISO/IEC 18367:2016	-	
IT Common Criteria security evaluation up to AVA_VAN.2 - Cryptographic analysis/ : Entropy analysis/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + ISO/IEC 20543:2019	-	
IT Common Criteria security evaluation up to AVA_VAN.2 - Cryptographic analysis/ : Security Assessment/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + ISO/IEC 20004:2015	-	
IT Common Criteria security evaluation up to AVA_VAN.2 - Vulnerability analysis/ : Bypass/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + ISO/IEC 20004:2015	-	
IT Common Criteria security evaluation up to AVA_VAN.2 - Vulnerability analysis/ : Code Injection/, Denial of service/, Direct attacks/, Exploit development/, Generational Fuzzing/, Generic vulnerability search/, Hooking attacks/, Memory dumps/, Meta characters encoding & Input validation/, Misuse/, Mutational fuzzing/, Overrun/, Protocol Attacks/, Public exploits application/, Race condition/, Tampering/, Web application security/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + OWASP	-	

ATSEC Information Security srl Via Santa Croce in Gerusalemme 63 00185 Roma RM	UNI CEI EN ISO/IEC 17025:2018
	Revisione: 0 Data: 22/10/2025
	Sede A pag. 2 di 2

ELENCO Prove Accreditate - Con Campo Fisso in Categoria: III

Applicative security/, Communication protocols/, Cryptographic Mechanisms/, Databases/, Embedded systems, microkernels/, Filtering/, Hardware components protocols/, Intrusion detection/, Low-level interfaces/, Network protocols/, Personal computer and server security/, Phone and VoIP/, State-of-the-art of Approved Cryptographic Mechanisms/, Virtualization/, Web technologies/, Wireless/, Mobile networks/

Denominazione della prova / Campi di prova	Metodo di prova	Tecnica di prova	O&I
IT Common Criteria security evaluation up to AVA_VAN.2 - Cryptographic analysis/ : Conformity analysis and tests/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + ISO/IEC 18367:2016	-	
IT Common Criteria security evaluation up to AVA_VAN.2 - Cryptographic analysis/ : Entropy analysis/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + ISO/IEC 20543:2019	-	
IT Common Criteria security evaluation up to AVA_VAN.2 - Cryptographic analysis/ : Security Assessment/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + ISO/IEC 20004:2015	-	
IT Common Criteria security evaluation up to AVA_VAN.2 - Vulnerability analysis/ : Bypass/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + ISO/IEC 20004:2015	-	
IT Common Criteria security evaluation up to AVA_VAN.2 - Vulnerability analysis/ : Code Injection/, Denial of service/, Direct attacks/, Exploit development/, Generational Fuzzing/, Generic vulnerability search/, Hooking attacks/, Memory dumps/, Meta characters encoding & Input validation/, Misuse/, Mutational fuzzing/, Overrun/, Protocol Attacks/, Public exploits application/, Race condition/, Tampering/, Web application security/ (ADV_ARC.1 + ADV_FSP.3 + ADV_TDS.2 + AGD_OPE.1 + AGD_PRE.1 + ALC_CMC.3 + ALC_CMS.3 + ALC_DEL.1 + ALC_DVS.1 + ALC_LCD.1 + ASE_CCL.1 + ASE_ECD.1 + ASE_INT.1 + ASE_OBJ.2 + ASE_REQ.2 + ASE_SPD.1 + ASE_TSS.1 + ATE_COV.2 + ATE_DPT.1 + ATE_FUN.1 + ATE_IND.2 + AVA_VAN.2 + ALC_FLR.3)	ISO/IEC 15408-1:2022 + ISO/IEC 15408-2:2022 + ISO/IEC 15408-3:2022 + ISO/IEC 15408-4:2022 + ISO/IEC 15408-5:2022 + ISO/IEC 18045:2022 + OWASP	-	

Legenda/Note

Il simbolo (1), se presente, indica: "Materiale/Prodotto/Matrice" non previsto dal metodo ma assimilabile/The symbol (1), if present, means: Material/Product/Matrix not provided for by the method but acceptable
 Per la definizione della "categoria" di prova indicata nel titolo, si veda il Regolamento Generale ACCREDIA RG-02/For the definition of the test "category" indicated in the title, see ACCREDIA General Regulation RG-02.

Il QRcode consente di accedere direttamente al sito www.accredia.it per verificare la validità dell'elenco prove e del certificato di accreditamento rilasciato al laboratorio/The QRcode allows to directly access to the website www.accredia.it to verify the validity of the test list and of the accreditation certificate issued to the laboratory.

L'eventuale simbolo "X" riportato nella colonna "O&I" indica che il laboratorio è accreditato anche per fornire opinioni e interpretazioni basate sui risultati delle specifiche prove contrassegnate/Any "X" symbol in the "O&I" column indicates that the laboratory is also accredited to provide opinions and interpretations based on the results of the specific marked tests.

L'eventuale simbolo (*) indica che è attiva una sospensione dell'accREDITAMENTO per la specifica attività riportata a fianco/Any symbol (*) indicates that a suspension of accreditation is active for the specific activity shown next to it.

