

CERTIFICAT

CERTIFICADO

СЕРТИФИКАТ

認證證書

CERTIFICATE

ZERTIFIKAT



Italia

CERTIFICATO

CERTIFICATE

Cybersecurity

Certificato No.:

Certificate No.:

TUV IT 25 CYB A 005

Nome ed indirizzo del fabbricante:

Name and address of manufacturer:

Exor International S.p.A.
Via Monte Fiorino, 13,
37057 San Giovanni Lupatoto (VR)
Italy

Sede/i:

Site:

See above

Processo:

Process:

Secure Development Lifecycle (SDL)

Modello/tipo:

Model/type:

SDL is defined in document CPRO 6.0
revision 1.1.

Parametri:

Parameters:

ML2 - See Annex for details

Rapporto di Valutazione:

Assessment report:

RC0769A-AR-GA-250619-01 v1.0

Si certifica che il processo soddisfa i requisiti della(e) norma(e):

We herewith certify that the process meets the requirements of the following standard(s):

IEC62443-4-1:2018

Data 1a emissione: 2025-07-31

First Issue date:

Data emissione: 2025-07-31

Issue date:

Data di scadenza: 2028-07-30

Expiry date:



00077 PRD
Membro degli Accordi di Mutuo Riconoscimento
EA, IAF e ILAC
Signatory of EA, IAF and ILAC Mutual
Recognition Agreements



TÜV Italia S.r.l.

Alberto Carelli
Industrie Service Division Manager



Allegato al Certificato
Annex to certificate
n° TUV IT 25 CYB A 005

Additional parameters: -

List of practices and requirements:

ID	Requirement	Maturity Level	Notes
Practice 1 - Security Management (SM)			
SM-1	Development process	2	
SM-2	Identification of responsibilities	2	
SM-3	Identification of applicability	2	
SM-4	Security expertise	2	
SM-5	Process scoping	2	
SM-6	File integrity	2	
SM-7	Development environment security	2	
SM-8	Controls for private keys	2	
SM-9	Security requirements for externally provided components	2	
SM-10	Custom developed components from third-party suppliers	2	
SM-11	Assessing and addressing security-related issues	2	
SM-12	Process verification	2	
SM-13	Continuous improvement	2	
SR-1	Product security context	2	
SR-2	Threat model	2	
SR-3	Product security requirements	2	
SR-4	Product security requirements content	2	
SR-5	Security requirements review	2	
SD-1	Secure design principles	2	
SD-2	Defense in depth design	2	
SD-3	Security design review	2	
SD-4	Secure design best practices	2	
SI-1	Security implementation review	2	
SI-2	Secure coding standards	2	
SVV-1	Security requirements testing	2	
SVV-2	Threat mitigation testing	2	
SVV-3	Vulnerability testing	2	
SVV-4	Penetration testing	2	
SVV-5	Independence of testers	2	
DM-1	Receiving notifications of security-related issues	2	
DM-2	Reviewing security-related issues	2	
DM-3	Assessing security-related issues	2	
DM-4	Addressing security-related issues	2	



ID	Requirement	Maturity Level	Notes
DM-5	Disclosing security-related issues	2	
DM-6	Periodic review of security defect management practice	2	
SUM-1	Security update qualification	2	
SUM-2	Security update documentation	2	
SUM-3	Dependent component or operating system security update documentation	2	
SUM-4	Security update delivery	2	
SUM-5	Timely delivery of security patches	2	
SG-1	Product defense in depth	2	
SG-2	Defense in depth measures expected in the environment	2	
SG-3	Security hardening guidelines	2	
SG-4	Secure disposal guidelines	2	
SG-5	Secure operation guidelines	2	
SG-6	Account management guidelines	2	
SG-7	Documentation review	2	

Notes: -