

PRASSI DI RIFERIMENTO

UNI/PdR 193

17 SETTEMBRE 2026

Requisiti e principi per la valutazione delle competenze digitali e la certificazione delle persone, in accordo alla UNI CEI EN ISO/IEC 17024, con riferimento ai framework Digital Competence Framework for Citizens (DigComp) e il Digital Competence Framework for Educators (DigCompEdu)

Requirements and principles for the assessment of digital competences and the certification of persons in accordance with UNI CEI EN ISO/IEC 17024, with reference to the Digital Competence Framework for Citizens (DigComp) and the Digital Competence Framework for Educators (DigCompEdu)

TESTO ITALIANO

ICS 35.020, 03.040

SOMMARIO

La prassi di riferimento definisce i requisiti e i principi per la valutazione delle competenze digitali e per la certificazione delle persone, in accordo alla UNI CEI EN ISO/IEC 17024, con riferimento al Digital Competence Framework for Citizens (DigComp) e al Digital Competence Framework for Educators (DigCompEdu) con l'obiettivo di promuovere trasparenza, coerenza e tracciabilità nei processi di valutazione della conformità andando ad individuare:

- i livelli di padronanza per le aree di competenza;
- le metodologie e gli ambiti di valutazione;
- gli indicatori di prestazione;
- i requisiti di processo per gli organismi che operano nell'ambito della valutazione della conformità.

PREMESSA

La prassi di riferimento è stata elaborata dal Tavolo UNI/PdR

Valutazione delle competenze digitali

La prassi di riferimento è stata ratificata dal Presidente dell'UNI ed entra in vigore il 17 settembre 2026.

*La prassi di riferimento è pubblicata in **versione accessibile**, ovvero può essere letta da persone con disabilità visive tramite il supporto di tecnologie assistive.*

© UNI

Riproduzione vietata ai sensi della Legge 22 aprile 1941 N° 633 e ss.mm.ii.

I contenuti del documento possono essere riprodotti o diffusi solo previa autorizzazione scritta di UNI.

Le prassi di riferimento UNI sono documenti tutelati da copyright pur essendo liberamente disponibili (in quanto preventivamente finanziate dalle parti interessate) previa registrazione.

Con l'utilizzo di questo documento (e con l'associazione a UNI) si partecipa al mantenimento e alla crescita di un sistema di autoregolamentazione che crea e tiene aggiornato lo stato dell'arte, a garanzia di una qualità disponibile e diffusa.

Le prassi di riferimento UNI sono prodotti della normazione elaborati grazie al contributo di coloro che hanno partecipato ai lavori, tutti i dettagli sull'iter sono riportati nella regolamentazione applicabile, disponibile sul sito www.uni.com (Chi Siamo - Documenti).

Si richiama l'attenzione sulla possibilità che alcuni degli elementi del presente documento possano essere oggetto di diritti di brevetto. UNI non deve essere ritenuto responsabile dell'identificazione di tali diritti di brevetto.

Le prassi di riferimento UNI sono riesaminate periodicamente e possono essere superate da nuove norme, pertanto è importante che l'utente si accerti di essere in possesso dell'edizione in vigore.

PREMESSA

La prassi di riferimento UNI/PdR 193:2026 non è una norma nazionale, ma è un documento pubblicato da UNI, come previsto dal Regolamento UE n. 1025/2012, che raccoglie prescrizioni relative a prassi condivise all'interno del seguente soggetto firmatario di un accordo di collaborazione con UNI:

IDCERT SRL SB

Via G. Pugnani, 1
76123 Andria (BT)

Fondazione Italia Digitale

Via dei Fossi, 1
50123 Firenze

La presente prassi di riferimento è stata elaborata dal Tavolo "Valutazione delle competenze digitali" condotto da UNI, costituito dai seguenti esperti:

- *Simone Aldo Buonporto – Project Leader (IDCERT)*
- *Francesco Di Costanzo (Fondazione Italia Digitale)*
- *Flavia Bulletti (FLC CGIL)*
- *Roberto Calienno (CISL Scuola)*
- *Paolo De Santis (Ministero dell'Istruzione e del Merito)*
- *Angelo Del Giudice (Accredia)*
- *Franco Fontana (ASSOTIC – Conforma – UN.I.O.N.)*
- *Stefano Kluzer (All Digital)*
- *Giancarlo Montico (IDCERT)*
- *Gerardo Perrone (IDCERT)*
- *Giovanni Renzi Brivio (UNI/CT 040 "Servizi")*
- *Emanuele Riva (Accredia)*
- *Antonio Romeo (Unioncamere)*
- *Monica Trippodo (Gruppo IQC-Pomiager)*
- *Altheo Valentini (EGInA)*

SOMMARIO

INTRODUZIONE	3
CONTESTO	3
ESIGENZA	3
1 SCOPO E CAMPO DI APPLICAZIONE	5
2 RIFERIMENTI NORMATIVI E LEGISLATIVI	5
3 TERMINI E DEFINIZIONI	6
4 PRINCIPIO	9
5 ELEMENTI PER LA VALUTAZIONE DELLA CONFORMITÀ	10
5.1 GENERALITÀ	10
5.2 DOMANDA DI CERTIFICAZIONE	10
5.3 MODALITÀ DI IDENTIFICAZIONE	11
5.4 ELEMENTI PER L'ACCESSO AL PROCESSO DI VALUTAZIONE DELLA CONFORMITÀ (ESAME DI CERTIFICAZIONE)	11
5.5 METODI DI VALUTAZIONE APPLICABILI	12
5.5.1 GENERALITÀ	12
5.5.2 SVOLGIMENTO DELLE PROVE DI ESAME	12
5.5.2.1 STRUTTURA DELLO SVOLGIMENTO	12
5.5.2.2 MODALITÀ D'ESAME	13
5.5.3 CARATTERISTICHE TECNICHE OBBLIGATORIE	15
5.5.3.1 GENERALITÀ	15
5.5.3.2 REQUISITI APPLICABILI A TUTTE LE MODALITÀ DI ESAME	16
5.5.3.3 REQUISITI PER ESAMI ONLINE DA REMOTO - LIVELLO MINIMO OBBLIGATORIO	17
5.5.3.4 REQUISITI PER ESAMI ONLINE DA REMOTO - LIVELLO AVANZATO OPZIONALE (SISTEMI AI)	18
5.5.3.5 REQUISITI PER ESAMI IN PRESENZA PRESSO SEDI SECONDARIE DELL'ODC	20
5.5.4 PROCESSO DI QUALIFICA DEGLI ESAMINATORI	21
5.5.5 PROCESSO DI QUALIFICA DEI PROCTOR (SORVEGLIANTI)	22
5.6 ELEMENTI PER IL MANTENIMENTO	22
5.7 ELEMENTI PER IL RINNOVO	22
5.8 RIFERIMENTO ALLA CERTIFICAZIONE E UTILIZZO DEL MARCHIO UNI	22
5.9 EMISSIONE DEI CERTIFICATI E RILASCIO OPEN BADGE DIGITALE	23
5.9.1 GENERALITÀ	23
5.9.2 CONTENUTO DEL CERTIFICATO	23
5.9.3 OPEN BADGE DIGITALE (OPZIONALE)	24
5.9.3.1 GENERALITÀ	24
5.9.3.2 STRUTTURA DELL'OPEN BADGE	24
5.9.3.3 FORMATO TECNICO	25
5.9.4 INTEROPERABILITÀ (OPZIONALE)	25
5.9.4.1 ALLINEAMENTO ALLO EUROPEAN LEARNING MODEL (ELM)	25
5.9.4.2 COMPATIBILITÀ EUROPASS	25
6 REQUISITI SUPPLEMENTARI PER PERSONE CON BISOGNI SPECIALI	26
APPENDICE A (INFORMATIVA)	
ESEMPI DI COMPORTAMENTI NON RACCOMANDATI	27
APPENDICE B (INFORMATIVA)	
ESEMPI DI CERTIFICATO E OPEN BADGE	30
BIBLIOGRAFIA	33

INTRODUZIONE

CONTESTO

I framework DigComp (Digital Competence Framework for Citizens), ora alla versione 3.0, e DigCompEdu (Digital Competence Framework for Educators), pubblicato nel 2017, sono strumenti elaborati dalla Commissione Europea e dal Joint Research Centre per fornire una base comune nella definizione, sviluppo e valutazione delle competenze digitali rispettivamente dei cittadini e degli educatori. In Italia, sono stati adottati e adattati da enti pubblici e privati a supporto delle politiche di digitalizzazione, della formazione e del riconoscimento delle competenze.

DigComp, nella sua versione attuale, individua 5 aree di competenza articolate in 21 competenze digitali rilevanti per tutti i cittadini, con un sistema di livelli da base ad altamente avanzato.

DigCompEdu declina queste competenze nel contesto dell'insegnamento e dell'apprendimento, suddividendole in 6 aree e 22 competenze, strutturate su sei livelli di padronanza (da A1 a C2).

Entrambi i framework non sono norme vincolanti, ma documenti guida di riferimento riconosciuti a livello europeo. Non costituiscono una "certificazione delle competenze" ai sensi del Decreto Legislativo (D.Lgs.) 13/2013, né un'attestazione ai sensi della Legge 4/2013, ma rappresentano una base per la certificazione volontaria di parte terza secondo la UNI CEI EN ISO/IEC 17024. La certificazione consente di attestare in modo trasparente, tracciabile e interoperabile le competenze digitali acquisite, valorizzandole nel mercato del lavoro, nella formazione e nella pubblica amministrazione.

Per approfondimenti:

- DigComp: https://joint-research-centre.ec.europa.eu/digcomp_en
- DigCompEdu: https://joint-research-centre.ec.europa.eu/digcompedu_en

ESIGENZA

La redazione di questa prassi nasce dall'esigenza di fornire un riferimento chiaro e condiviso per la valutazione della conformità dei percorsi di certificazione che si basano sui framework DigComp e DigCompEdu. Tali framework, infatti, non hanno natura normativa e non contengono indicazioni operative su come strutturare processi valutativi conformi alla norma UNI CEI EN ISO/IEC 17024. Questa assenza ha portato alla proliferazione di iniziative non uniformi tra loro, con significative divergenze nei criteri di esame, nella costruzione delle prove e nella gestione dei processi di certificazione.

Ad oggi, organismi accreditati e non accreditati propongono certificazioni riferite ai medesimi framework, ma spesso con modalità e strutture profondamente diverse, generando confusione nel mercato e mettendo a rischio la credibilità dell'intero sistema, con ripercussioni verso le Istituzioni pubbliche e private che si riferiscono alle persone certificate.

In questo contesto, Accredia – l'Ente unico nazionale di accreditamento – assume un ruolo cruciale nel garantire l'affidabilità, l'imparzialità e la tracciabilità del processo, promuovendo l'applicazione coerente della UNI CEI EN ISO/IEC 17024 e vigilando sulla corretta implementazione degli schemi.

Nel 2025, lo scenario normativo italiano contribuisce ulteriormente all'importanza di questa prassi: bandi pubblici (come, ad esempio, quelli legati alle Graduatorie ATA), il Decreto Ministeriale 115/2024, CCNL Scuola 2019-2021 e altri provvedimenti incentivano o premiano il possesso di certificazioni basate su DigComp, senza tuttavia definire standard minimi condivisi.

A livello tecnologico e strategico, l'interoperabilità dei certificati rappresenta un obiettivo centrale: la convergenza verso strumenti come IT Wallet e l'identità digitale unica europea impone che le certificazioni siano leggibili, validate e riconoscibili in ambienti digitali interoperabili.

In tale ottica, la prassi propone requisiti che contribuiscono alla digitalizzazione sicura, all'integrità del dato e alla trasparenza verso cittadini, pubbliche amministrazioni ed enti formativi.

In Italia e in Europa si osserva oggi una crescente richiesta di certificazioni di competenze digitali, sia per cittadini che per educatori. Tuttavia, l'assenza di una norma cogente o di una prassi condivisa ha favorito l'emergere di scenari molto eterogenei. Sul territorio italiano coesistono:

- organismi accreditati secondo UNI CEI EN ISO/IEC 17024 che strutturano esami basati su criteri oggettivi, progressivi e tracciabili, con piattaforme validate e personale qualificato;
- enti non accreditati che offrono certificazioni con accesso libero, modalità d'esame semplificate o automatizzate, talvolta senza adeguate garanzie di identità, imparzialità o tracciabilità;
- offerte commerciali ibride che combinano formazione e certificazione, con percorsi a pagamento spesso finalizzati alla partecipazione a graduatorie o bandi pubblici, ma senza garanzie sull'effettiva valutazione delle competenze.

A livello europeo, gran parte degli Stati membri hanno avviato iniziative pubbliche basate sul DigComp come base per programmi di upskilling e reskilling. Tuttavia, salvo eccezioni, la certificazione delle competenze resta prevalentemente affidata a iniziative locali o private, non coordinate tra loro, riproducendo una frammentazione analoga a quella italiana [2].

In questo contesto frammentato, sia a livello nazionale che europeo, diventa essenziale stabilire criteri comuni per l'accesso alla certificazione, che garantiscano:

- l'identificazione certa del candidato;
- l'equità dell'accesso anche per soggetti con bisogni speciali;
- l'indipendenza tra formazione ed esame;
- la qualità, imparzialità e tracciabilità delle prove.

Il perseguimento di questi criteri non può prescindere dall'adozione di piattaforme digitali interoperabili, l'impiego di tecnologie di identificazione sicura (SPID, CIE, IT Wallet) e la convergenza verso formati standardizzati per il riconoscimento dei certificati (per esempio Europass, Digital Credentials, micro-credentials), le quali rappresentano le leve principali per assicurare l'equità e l'affidabilità dei processi su scala nazionale ed europea.

1 SCOPO E CAMPO DI APPLICAZIONE

La prassi di riferimento definisce i requisiti e i principi per la valutazione di conformità delle competenze digitali, per la certificazione delle persone, in accordo alla UNI CEI EN ISO/IEC 17024, con riferimento al Digital Competence Framework for Citizens (DigComp) e al Digital Competence Framework for Educators (DigCompEdu) con l'obiettivo di promuovere indipendenza, imparzialità, uniformità, trasparenza, coerenza e tracciabilità nei processi di valutazione della conformità andando ad individuare:

- i livelli di padronanza per le aree di competenza;
- le metodologie e gli ambiti di valutazione;
- gli indicatori di prestazione;
- i requisiti di processo per gli organismi che operano nell'ambito della valutazione della conformità;
- i requisiti prestazionali e le caratteristiche tecniche della piattaforma di esame.

NOTA: Si precisa che, trattandosi di framework riferiti alle persone intese come “cittadini” o “educatori”, non si tratta di professionisti intesi come da definizione e contesto della Legge 4/2013. Il contesto è da intendersi per entrambi i framework come una certificazione di persone non professionale e non basata su prerequisiti di ingresso di alcune genere.

2 RIFERIMENTI NORMATIVI E LEGISLATIVI

La presente prassi di riferimento rimanda, mediante riferimenti datati e non, a disposizioni contenute in altre pubblicazioni. Tali riferimenti normativi e legislativi sono citati nei punti appropriati del testo e sono di seguito elencati. Per quanto riguarda i riferimenti datati, successive modifiche o revisioni apportate a dette pubblicazioni valgono unicamente se introdotte nel presente documento come aggiornamento o revisione. Per i riferimenti non datati vale l'ultima edizione della pubblicazione alla quale si fa riferimento.

- UNI CEI EN ISO/IEC 17024 Valutazione della conformità - Requisiti generali per gli organismi che eseguono la certificazione di persone
- ISO CASCO Guidance of ISO/IEC 17024
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, “Protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”
- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, “Regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)”
- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, “in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE” (eIDAS)
- Decreto Legislativo 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali”, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016

- Decreto Legislativo 10 agosto 2018, n. 101, “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE”
- Legge 23 settembre 2025, n. 132, “Disposizioni e deleghe al Governo in materia di intelligenza artificiale”
- Legge 9 gennaio 2004, n. 4, “Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici”

3 TERMINI E DEFINIZIONI

Ai fini del presente documento valgono i termini e le definizioni seguenti:

3.1

abilità:

Capacità di applicare conoscenze (3.8) e di usare il know-how per portare a termine compiti e risolvere problemi.

NOTA: Nel contesto dello EQF (European Qualifications Framework) e del QNQ (Quadro Nazionale delle Qualificazioni) le abilità sono descritte come cognitive (comprendenti l'uso del pensiero logico, intuitivo e creativo) o pratiche (comprendenti la manualità e l'uso di metodi, materiali, strumenti e utensili).

[FONTE: EQF, Allegato I, definizione g)]

3.2

apprendimento formale:

Apprendimento che si attua nel sistema di istruzione e formazione e nelle università e istituzioni di alta formazione artistica, musicale e coreutica, e che si conclude con il conseguimento di un titolo di studio o di una qualifica o diploma professionale, conseguiti anche in apprendistato, o di una certificazione riconosciuta, nel rispetto della legislazione vigente in materia di ordinamenti scolastici e universitari.

NOTA: La definizione è quella riportata nel D.Lgs. 13/2013, Articolo 2, comma 1, lettera b), ed è coerente con [5].

3.3

apprendimento informale:

Apprendimento che, anche a prescindere da una scelta intenzionale, si realizza nello svolgimento, da parte di ogni persona, di attività nelle situazioni di vita quotidiana e nelle interazioni che in essa hanno luogo, nell'ambito del contesto di lavoro, familiare e del tempo libero.

NOTA: La definizione è quella riportata nel D.Lgs. 13/2013, Articolo 2, comma 1, lettera d), ed è coerente con [5].

3.4

apprendimento non-formale:

Apprendimento caratterizzato da una scelta intenzionale della persona, che si realizza al di fuori dei sistemi di cui all'apprendimento formale (3.2), in ogni organismo che persegua scopi educativi e formativi, anche del volontariato, del servizio civile nazionale e del privato sociale e nelle imprese.

NOTA: La definizione è quella riportata nel D.Lgs. 13/2013, Articolo 2, comma 1, lettera c), ed è coerente con [5].

3.5

autonomia e responsabilità:

Capacità della persona di applicare conoscenze (3.8) e abilità (3.1) in modo autonomo e responsabile.

3.6

centro d'esami:

Organizzazione qualificata dall'organismo di certificazione alla quale viene subappaltata almeno l'attività di esecuzione e gestione degli esami, che deve operare sotto il controllo e secondo le specifiche/procedure emesse dall'OdC e assicurare la propria imparzialità nei confronti di ogni candidato.

NOTA 1: Il centro d'esami non emette certificazioni, come previsto dalla UNI CEI EN ISO/IEC 17024.

NOTA 2: La presente prassi non ammette la possibilità di subappaltare l'attività d'esame ai centri d'esame, come specificato al punto 4 della presente prassi.

3.7

competenza:

Comprovata capacità di utilizzare conoscenze (3.8), abilità (3.1) e capacità personali, sociali e/o metodologiche in situazioni di lavoro o di studio e nello sviluppo professionale e personale.

[FONTE: EQF, Allegato I, definizione i)]

3.8

conoscenze:

Risultato dell'assimilazione di informazioni attraverso l'apprendimento.

NOTA 1: Le conoscenze sono l'insieme di fatti, principi, teorie e pratiche che riguardano un ambito di lavoro o di studio.

NOTA 2: Nel contesto dello EQF e del QNQ le conoscenze sono descritte come teoriche e/o pratiche.

[FONTE: EQF, Allegato I, definizione f)]

3.9

esame (di certificazione):

Insieme di attività che fanno parte della valutazione e che permettono di misurare la competenza (3.7) di un/a candidato/a mediante uno o più mezzi quali prove scritte, orali, pratiche od osservazione diretta.

[FONTE: UNI CEI EN ISO/IEC 17024 – con modifiche]

3.10

esaminatore/esaminatrice:

Persona che ha la competenza (3.7) per progettare il materiale d'esame (3.9), condurre un esame e valutarne i risultati.

[FONTE: UNI CEI EN ISO/IEC 17024 – con modifiche]

3.11

risultati dell'apprendimento:

Descrizione di ciò che una persona conosce, capisce ed è in grado di realizzare al termine di un processo di apprendimento.

NOTA 1: I risultati sono descritti in termini di conoscenze (3.8), abilità (3.1) e autonomia e responsabilità (3.5).

NOTA 2: I risultati dell'apprendimento possono derivare da contesti di apprendimenti formali, non formali o informali.

3.12

sorvegliante (proctor/invigilator):

Persona autorizzata dall'organismo di valutazione della conformità che gestisce o sovrintende a un esame (3.9), ma che non valuta la competenza (3.7) del/della candidato/a.

[FONTE: UNI CEI EN ISO/IEC 17024]

NOTA: Altri termini per "sorvegliante" sono: "addetto/a all'esame", "gestore dell'esame", "supervisore".

3.13

valutazione della conformità:

Dimostrazione che i requisiti specificati sono soddisfatti.

[FONTE: UNI CEI EN ISO/IEC 17000:2020, 4.1, modifica - Le note sono state eliminate]

3.14

Organismo di Certificazione (OdC):

Organismo (detto anche "di parte terza") che esegue attività di valutazione della conformità delle persone.

[FONTE UNI EN ISO/IEC 17000:2020, 4.6, modificata]

3.15

certificazione di terza parte:

Attestazione di terza parte, relativa a un oggetto di valutazione della conformità (3.13).

[FONTE UNI EN ISO/IEC 17000:2020, 7.6, modificata]

3.16

Know Your Customer (KYC):

Processo di verifica dell'identità del candidato condotto interamente da remoto tramite piattaforma digitale, in fase di registrazione e presentazione della domanda di certificazione, preliminarmente e in modo distinto rispetto alla sessione d'esame. Il processo prevede almeno:

- l'acquisizione e la verifica automatizzata del documento di identità del candidato;
- il confronto in tempo reale tra l'immagine del candidato acquisita dalla piattaforma e la fotografia presente sul documento di identità;
- il rilevamento della presenza fisica del candidato (liveness detection);
- la generazione di un log di verifica immutabile e conservabile.

3.17

micro-credenziali:

Registrazione (*record*) dei risultati di apprendimento che un partecipante ha conseguito a seguito di un piccolo "volume di apprendimento" (un corso breve, un modulo, un'attività formativa di durata contenuta). Le esperienze formative che conducono a una micro-credenziale sono finalizzate a fornire conoscenze, abilità e competenze specifiche, rispondendo a esigenze di natura sociale, culturale, personale o del mercato del lavoro. Le micro-credenziali sono di proprietà del soggetto che le consegue, sono potenzialmente cumulabili o combinabili per formare credenziali più ampie, e, laddove previsto, sono soggette a garanzia di qualità basata su standard appropriati per il settore di riferimento.

Una micro-credenziale basata su framework di competenze (DigCompd e DigCompEdu) definisce un *learning outcome* che corrisponde a una o più competenze del framework stesso; certifica che il titolare ha acquisito concretamente quella competenza, tramite un percorso formativo breve e verificabile.

NOTA: Nel contesto della presente prassi, non è previsto il rilascio di micro-credenziali relative a singoli livelli di padronanza o aree di competenza dei framework DigComp e DigCompEdu, in quanto l'esame deve essere sostenuto nella sua interezza (si rimanda al punto 5.5.2).

3.18

credenziali digitali (digital credential):

Rappresentazione digitale (in formato elettronico) di una credenziale o attestazione di apprendimento o competenza. Essa funge da mezzo tecnico per rilasciare, conservare, condividere e verificare credenziali (anche micro-credenziali) in modo sicuro e interoperabile.

NOTA: Una *digital credential* può includere metadati quali: identificazione del beneficiario, ente erogatore, data di rilascio, contenuto dell'apprendimento attestato, modalità di valutazione, e altri elementi informativi utili alla verifica e all'autenticità della credenziale.

3.19

scenario applicativo di valutazione della competenza:

Scenario di valutazione della singola competenza, basato sui risultati di apprendimento e sui descrittori dei livelli di padronanza definiti nel framework di riferimento applicabile.

4 PRINCIPIO

La prassi di riferimento si propone come un modello che fornisca agli Organismi di Certificazione (OdC) tutti i requisiti necessari per poter condurre l'esame di certificazione, secondo i framework DigComp e DigCompEdu.

Il documento delinea pertanto:

- le modalità e i requisiti di accesso all'esame di certificazione,
- le modalità di conduzione dell'intero processo dell'esame di certificazione da parte dell'OdC,
- le modalità di valutazione della prova di esame,
- le caratteristiche tecniche necessarie per lo svolgimento dell'esame,
- la tracciabilità dell'intero processo di certificazione, dall'identificazione del candidato alla delibera e all'emissione del certificato,
- i processi di qualifica degli esaminatori e dei proctor,
- il contenuto del certificato e/o dell'Open Badge Digitale, e
- i requisiti supplementari per garantire la fruibilità dell'esame alle persone con bisogni speciali.

L'Organismo di Certificazione accreditato deve mantenere la piena responsabilità e il controllo diretto dell'intero processo di certificazione. In particolare, l'Organismo deve garantire il presidio diretto delle attività critiche: progettazione e validazione delle prove, pianificazione e gestione delle sessioni d'esame, supervisione dello svolgimento, gestione e sicurezza delle piattaforme informatiche, validazione finale dei risultati.

Tali attività non possono essere delegate, esternalizzate o trasferite a soggetti terzi, centri affiliati, test center o strutture convenzionate che operino con autonomia organizzativa, operativa, decisionale o commerciale.

Non è ammessa la costituzione di filiere distributive o commerciali autonome per la promozione o la vendita delle certificazioni attraverso reti di test center o soggetti intermediari.

Il modello organizzativo deve assicurare che l'intera catena decisionale e operativa rimanga sotto il diretto controllo dell'OdC accreditato.

Eventuali sedi secondarie possono essere utilizzate esclusivamente come supporto logistico, nel rispetto di procedure formalizzate e sotto la piena responsabilità dell'OdC, ad esclusione delle Pubbliche Amministrazioni, con la condizione che le stesse siano censite all'interno del portale IndicePA.

NOTA: I gestori di pubblico servizio non rientrano nella categoria sopra citata.

Il sistema di certificazione delle competenze digitali deve essere progettato e gestito in modo da garantire la qualità, l'affidabilità e la sostenibilità organizzativa del processo certificativo, in coerenza con i principi della UNI CEI EN ISO/IEC 17024 e con il sistema nazionale di accreditamento.

Le modalità organizzative di erogazione delle certificazioni devono assicurare che il processo di valutazione sia svolto secondo adeguati standard di progettazione delle prove, gestione delle piattaforme informatiche di esame, supervisione delle sessioni di valutazione e controllo dei risultati, tali da preservare l'integrità, la tracciabilità e la credibilità delle certificazioni emesse.

Infine, la prassi di riferimento riporta, all'interno dell'appendice A, degli esempi di comportamenti non conformi alla presente prassi.

5 ELEMENTI PER LA VALUTAZIONE DELLA CONFORMITÀ

5.1 GENERALITÀ

Il presente punto specifica i requisiti per la valutazione della conformità relativa ai risultati dell'apprendimento, con puntuale riferimento al processo di certificazione di terza parte, in conformità alla UNI CEI EN ISO/IEC 17024, di cui mira ad assicurare una sempre maggiore uniformità e trasparenza.

NOTA: Si ricorda che il processo di certificazione di terza parte non è da confondersi con la "certificazione delle competenze" di cui al D.Lgs. 13/2013, processo ad appannaggio esclusivo degli "Enti titolati".

5.2 DOMANDA DI CERTIFICAZIONE

L'accesso al processo di valutazione della conformità deve avvenire mediante la presentazione digitale operata esclusivamente online attraverso il portale dell'OdC, che ospita l'intero ciclo di certificazione. Salvo specifiche e motivate esigenze di accessibilità per candidati con disabilità – da documentare e autorizzare secondo le procedure dell'OdC – non devono essere utilizzati moduli cartacei o modalità offline.

L'OdC deve disporre di procedure documentate per la gestione della continuità operativa della piattaforma, al fine di garantire l'accesso al processo di certificazione anche in caso di indisponibilità temporanea del portale, con tempestiva comunicazione ai candidati interessati.

La piattaforma, i cui requisiti tecnici sono specificati al punto 5.5.3, deve garantire l'identificazione univoca e sicura del candidato attraverso sistemi nazionali di identità digitale avanzata conformi al regolamento eIDAS, quali SPID/eIDAS e CIE.

Qualora non fosse possibile utilizzare i suddetti sistemi, l'OdC può applicare un processo alternativo di verifica dell'identità (per esempio KYC - Know Your Customer) che deve essere parimenti robusto, documentato e tracciabile, e deve essere preventivamente approvato nell'ambito del sistema di gestione per la conformità alla UNI CEI EN ISO/IEC 17024.

Il processo KYC deve essere condotto nel rispetto della normativa vigente in materia di protezione dei dati personali. Non è ammesso lo svolgimento del processo KYC in presenza fisica, in forma cartacea.

Il processo alternativo di cui sopra è applicabile, in particolare, ai candidati che non dispongano di un sistema di identità digitale notificato ai sensi del Regolamento (UE) 910/2014 (eIDAS), così da garantire l'accessibilità transfrontaliera del processo a parità di affidabilità della verifica.

La domanda di certificazione deve contenere almeno:

- dati anagrafici completi del candidato;
- codice fiscale o identificativo nazionale equivalente;
- campo di applicazione della certificazione (DigComp o DigCompEdu);
- presa visione dell'informativa sul trattamento dei dati personali, redatta nel rispetto del Regolamento UE 2016/679 (GDPR) e della normativa nazionale vigente;
- presa visione e accettazione digitale del regolamento, delle condizioni economiche, delle modalità di esame, delle procedure di ricorso e del codice etico;
- eventuale richiesta di misure compensative per situazioni particolari (DSA, disabilità, maternità, altre fragilità). Si rimanda anche al punto 6.

La conferma dell'invio della domanda e l'ammissione al processo di certificazione devono essere comunicate al candidato (es. tramite e-mail o notifica), registrate e consultabili all'interno della piattaforma, con data e registro di controllo associato.

L'OdC non deve accettare il trasferimento della certificazione da un altro OdC.

NOTA: Ai sensi del punto 5.4 della presente prassi, non essendo previsti requisiti minimi di accesso al processo di valutazione della conformità, il riesame della domanda di cui alla UNI CEI EN ISO/IEC 17024 si intende limitato alla verifica della completezza dei dati, dell'avvenuta identificazione digitale e dell'accettazione delle condizioni d'esame.

5.3 MODALITÀ DI IDENTIFICAZIONE

Il/la candidato/a deve essere identificato in modo certo e tracciabile attraverso un sistema digitale sicuro, prima dell'accesso all'esame di certificazione.

Tale identificazione deve avvenire tramite piattaforma digitale, mediante:

- SPID (Sistema Pubblico di Identità Digitale),
- CIE (Carta di Identità Elettronica),
- eIDAS (Electronic Identification, Authentication and Trust Services), oppure
- sistema KYC (Know Your Customer),

al fine di garantire l'identificazione certa del candidato. Le procedure di riconoscimento della persona fisica prima dell'accesso alla prova d'esame sono riportate al punto 5.5.3.2, lettera c), e si applicano a tutti i candidati, indipendentemente dal sistema di identificazione utilizzato.

La piattaforma deve conservare in modo sicuro i log di identificazione, collegando in modo univoco l'identità digitale verificata con l'account utilizzato per lo svolgimento della prova.

5.4 ELEMENTI PER L'ACCESSO AL PROCESSO DI VALUTAZIONE DELLA CONFORMITÀ (ESAME DI CERTIFICAZIONE)

Non sono previsti requisiti minimi di accesso al processo di valutazione della conformità. Il processo di certificazione deve essere consentito a candidati maggiorenni e minorenni. L'età minima ammessa è di quattordici anni.

Per i candidati minorenni, la domanda di certificazione deve essere integrata con l'autorizzazione esplicita di chi esercita la responsabilità genitoriale, ai sensi del Codice Civile.

Qualora l'identificazione del candidato minorenne avvenga tramite sistemi che prevedono un meccanismo integrato di autorizzazione parentale (per esempio SPID minorenni, CIE), tale meccanismo soddisfa il presente requisito. Qualora l'identificazione avvenga tramite processo KYC, la piattaforma dell'OdC deve acquisire e conservare l'autorizzazione di chi esercita la responsabilità genitoriale attraverso una procedura digitale documentata e tracciabile, prima della presentazione della domanda di esame.

5.5 METODI DI VALUTAZIONE APPLICABILI

5.5.1 GENERALITÀ

La valutazione deve avvenire esclusivamente mediante esame costituito da domande a risposta multipla e strutturato online sulla piattaforma digitale dell'OdC, senza alcun supporto cartaceo, rivolto a profili utente ("USER"). L'esame può essere svolto da remoto ovvero presso sedi secondarie dell'Organismo di Certificazione, sempre tramite la medesima piattaforma digitale e nel rispetto di tutti i requisiti previsti al punto 5.5.3.

5.5.2 SVOLGIMENTO DELLE PROVE DI ESAME

5.5.2.1 STRUTTURA DELLO SVOLGIMENTO

L'esame deve essere articolato in step con difficoltà incrementale, ciascuno dei quali deve essere superato per accedere al successivo. Il superamento deve essere regolato da soglie minime e massime di correttezza per ogni step. Ogni esame deve essere svolto in un'unica sessione continua: non deve essere consentita l'interruzione tra uno step e l'altro, né il frazionamento in più sessioni distinte. Non deve essere possibile condurre sessioni d'esame per singolo livello di padronanza e/o per singola area di competenza.

Gli step previsti per il DigComp devono essere:

- step 1 (livello base),
- step 2 (livello intermedio),
- step 3 (livello avanzato),
- step 4 (livello altamente avanzato).

NOTA: Rispetto al DigComp 2.2, i livelli base 1 e 2, intermedio 3 e 4, avanzato 5 e 6 e altamente avanzato 7 e 8, sono mappati nel DigComp 3.0 nei nuovi 4 livelli sopra riportati.

Di seguito, si riporta un prospetto comparativo, che riconduce i livelli di competenza DigComp alla classificazione Europass nei livelli da A1 a C2.

Prospetto 1 – Tabella di parcellizzazione dei livelli del DigComp 3.0 con il DigComp 2.2 e altri sistemi di mappatura (EQF, Europass, CEFR-like)

DigComp 3.0 Livelli ufficiali (4)	DigComp 2.2 Livelli ufficiali (8)	Mappatura alternativa Livelli A1-C2
Base	1	A1
Base	2	A2
Intermedio	3	B1
Intermedio	4	B2
Avanzato	5	C1
Avanzato	6	C1
Altamente avanzato	7	C2
Altamente avanzato	8	C2

NOTA: Per ragioni di accessibilità del documento, nella prima e terza colonna sono ripetuti rispettivamente i livelli:

- base, intermedio, avanzato e altamente avanzato, e
- C1 e C2.

La mappatura sopra riportata può essere inserita nel certificato di competenza del DigComp, evidenziando il livello ottenuto a seguito dell'esame.

NOTA: La segmentazione dei livelli di competenza proposta nel prospetto 01 (riportata anche a pagina 83 del DigComp 3.0) risponde alla necessità di rendere DigComp 3.0 pienamente interoperabile con DigComp 2.2 e con altri sistemi europei di riferimento (EQF, Europass, CEFR-like). L'articolazione in livelli più fini permette di descrivere in modo più preciso il livello di autonomia, complessità del compito e padronanza delle competenze digitali, migliorando l'affidabilità delle valutazioni e la comparabilità dei risultati. Tale struttura è inoltre funzionale alla progettazione di micro-credenziali e percorsi formativi modulari, in quanto offre un modello di progressione chiaro e misurabile, utile sia ai formatori sia agli enti certificatori.

Gli step previsti per il DigCompEdu devono essere:

- step 1 (livello A1-A2)
- step 2 (livello B1-B2)
- step 3 (livello C1-C2).

L'esame deve essere sempre sostenuto nella sua interezza e non devono essere ammesse forme di compensazione o riduzione del processo d'esame.

NOTA: La struttura è *user-centrica* con focus sulla progressione personale e non è basata su requisiti di ruolo o status professionale, e come indicato dai Framework è aperta a tutti i cittadini ed educatori.

5.5.2.2 MODALITÀ D'ESAME

Gli organismi che eseguono la valutazione della conformità dei risultati dell'apprendimento devono effettuare quanto segue:

- 1) L'esame deve essere strutturato in più step progressivi, con difficoltà incrementale. Se il candidato non supera uno step, il processo deve essere interrotto e deve essere certificato il livello precedentemente raggiunto e superato.
- 2) L'esame deve consistere in una prova con domande a risposta multipla basate su scenari applicativi conformi:
 - per il DigComp, ai risultati di apprendimento strutturati secondo i descrittori di Conoscenza (Knowledge), Abilità (Skill) e Atteggiamento (Attitude) del framework;
 - per il DigCompEdu, ai descrittori dei livelli di padronanza definiti nel framework.

Per ogni domanda devono essere proposte almeno 4 risposte delle quali 1 sola è corretta (da escludere quelle del tipo "vero/falso"). L'OdC può prevedere un numero superiore di opzioni di risposta. Ciascuno step è composto da almeno 1 domanda per ogni competenza (21 per DigComp e 22 per DigCompEdu), per ciascuno dei livelli (4 per il DigComp e 6 per il DigCompEdu) oggetto della prova di esame. Pertanto, si identificano almeno 84 domande per DigComp e 132 per DigCompEdu.

NOTA: Si ricorda che i livelli complessivi per DigComp sono base, intermedio, avanzato e altamente avanzato, mentre quelli per il DigCompEdu sono A1-A2, B1-B2 e C1-C2.

- 3) L'esame DigComp è strutturato in 4 step progressivi e ha una durata massima consigliata di almeno 120 minuti. La piattaforma gestisce la chiusura automatica dell'esame allo scadere del tempo. Le soglie di valutazione degli step devono essere distribuite come riportato di seguito:
- Step 1 – Livello Base:
 - $\leq 25\%$ delle risposte corrette, l'esame viene considerato Respinto
 - con percentuale tra 25,01% e 74,99%, per ciascuna area di competenza: viene attestato il Livello Base
 - $\geq 75\%$: il candidato procede allo Step 2.
 - Step 2 – Livello Intermedio:
 - $\leq 50\%$: viene attestato il Livello Base
 - con percentuale tra 50,01% e 74,99%: viene attestato il Livello Intermedio
 - $\geq 75\%$: il candidato procede allo Step 3.
 - Step 3 – Livello Avanzato:
 - $\leq 50\%$: viene attestato il Livello Intermedio
 - con percentuale tra 50,01% e 74,99%: viene attestato il Livello Avanzato
 - $\geq 75\%$: il candidato procede allo Step 4.
 - Step 4 – Livello Altamente Avanzato:
 - $\leq 75\%$: viene attestato il Livello Avanzato
 - con percentuale tra 75,01% e 100%: viene attestato il Livello Altamente Avanzato (massimo livello conseguibile).
- 4) L'esame DigCompEdu è strutturato in 3 step progressivi e ha una durata massima consigliata di almeno 190 minuti. Le soglie di valutazione degli step devono essere distribuite come riportato di seguito:
- Step 1:
 - $\leq 25\%$ delle risposte corrette, l'esame viene considerato Respinto
 - con percentuale tra 25,01% e 50%, per ciascuna area di competenza: viene attestato il livello A1
 - con percentuale tra 50,01% e 74,99%: viene attestato il livello A2
 - superando il 75%: si procede allo Step 2.

- Step 2:
 - $\leq 25\%$ delle risposte corrette: si mantiene il livello A2
 - con percentuale tra 25,01% e 50%: viene attestato il livello B1
 - con percentuale tra 50,01% e 74,99%: viene attestato il livello B2
 - superando il 75%: procede allo Step 3.
- Step 3:
 - $\leq 25\%$ delle risposte corrette: si mantiene il livello B2
 - con percentuale tra 25,01% e 75%: viene attestato il livello C1
 - con percentuale $\geq 75,01\%$: viene attestato il livello C2 (massimo livello conseguibile).

Questa struttura garantisce una progressione coerente e trasparente del livello di competenza, in linea con i principi di validità, equità e imparzialità previsti dagli standard di certificazione delle competenze.

NOTA: La differente articolazione delle soglie tra DigComp e DigCompEdu è determinata dalla struttura dei rispettivi step: nel DigComp ciascuno step corrisponde a un singolo livello di padronanza, nel DigCompEdu ciascuno step comprende due livelli.

In caso di interruzione della sessione d'esame dovuta a comprovati problemi tecnici della piattaforma, l'OdC deve prevedere un protocollo documentato di riprogrammazione della sessione, senza penalizzazione per il candidato. Tale protocollo deve essere previsto nell'ambito del sistema di gestione dell'OdC.

5.5.3 CARATTERISTICHE TECNICHE OBBLIGATORIE

5.5.3.1 GENERALITÀ

I seguenti requisiti inerenti alle caratteristiche tecniche sono finalizzati alla prevenzione delle frodi e alla garanzia dell'integrità, tracciabilità e imparzialità del processo certificativo.

I requisiti di sorveglianza per gli esami svolti online da remoto sono articolati su due livelli:

- **livello minimo obbligatorio** (punto 5.5.3.2): sorveglianza tramite webcam con controllo umano in tempo reale
- **livello avanzato opzionale** (punto 5.5.3.4): utilizzo di sistemi di monitoraggio basati su intelligenza artificiale, in aggiunta ai requisiti del livello minimo.

Il seguente prospetto 2 sintetizza i rapporti massimi tra proctor e candidati per ciascuna modalità.

Prospetto 2 – Rapporto massimo tra proctor e candidati

Modalità di esame	Rapporto massimo tra proctor e candidati	Riferimento
In presenza (sede secondaria OdC)	1 proctor ogni 30 candidati	Punto 5.5.3.5, lettera b)
Online da remoto - Livello minimo	1 proctor ogni 50 candidati	Punto 5.5.3.3, lettera d)
Online da remoto - Livello avanzato (AI)	1 proctor ogni 500 candidati	Punto 5.5.3.4, lettera f)

5.5.3.2 REQUISITI APPLICABILI A TUTTE LE MODALITÀ DI ESAME

I seguenti requisiti devono essere rispettati indipendentemente dalla modalità di svolgimento dell'esame (da remoto o in presenza):

- a) tracciamento integrale del processo d'esame: la piattaforma deve garantire il tracciamento integrale del processo d'esame, inclusi:
 - i. il monitoraggio del tempo;
 - ii. il blocco dei tentativi multipli di sostenimento dell'esame (1 tentativo al giorno consentito);
 - iii. la randomizzazione delle domande e risposte e la generazione automatica dell'esito;
- b) verifica tecnica dei dispositivi del candidato: deve essere effettuata la verifica tecnica dei dispositivi (hardware) del candidato prima dell'accesso alla sala d'attesa. In particolare:
 - i. microfono (per comunicare con il supervisore);
 - ii. webcam (per il monitoraggio durante l'esame);
 - iii. audio (per ascoltare le istruzioni);
 - iv. connessione (per garantire stabilità durante l'esame);
- c) autenticazione e riconoscimento:
 - i. autenticazione tramite SPID/CIE/eIDAS o sistema KYC, conformemente a quanto previsto ai punti 5.2 e 5.3 della presente prassi;
 - ii. riconoscimento del candidato da parte del proctor umano mediante confronto visivo in tempo reale tra il candidato (via webcam o in presenza) e il documento di identità, al fine di verificare che la persona che accede alla sessione d'esame corrisponda al candidato identificato. Tale operazione non comporta l'estrazione o il trattamento di dati biometrici;
 - iii. conferma di assenza di conflitto di interessi tra proctor e singolo candidato;
- d) logging e tracciabilità:
 - i. log automatico di: accessi (modalità connessione e identificazione), eventi sospetti, interventi del proctor, tentativi di frode;
 - ii. conservazione dei log per la durata di validità del certificato (2 anni);
 - iii. conservazione dei video (se registrati) almeno fino a delibera o per 30 giorni;
 - iv. collegamento tra: identità verificata del candidato, proctor della sessione d'esame, sessione d'esame e risultato conseguito;

- e) misure di emergenza e segnalazione:
 - i. pulsante (per esempio richiedi assistenza) con apertura canale live con proctor;
 - ii. sistema di alert automatico di log in caso di anomalie;
 - iii. protocollo di riprogrammazione in caso di problemi tecnici validati, come specificato al punto 5.5.2.2;
- f) risultato dell'esame:
 - il risultato finale non granulare deve essere riportato al candidato alla fine dell'esame;
- g) validazione della piattaforma:
 - la piattaforma deve essere validata dall'OdC.

5.5.3.3 REQUISITI PER ESAMI ONLINE DA REMOTO - LIVELLO MINIMO OBBLIGATORIO

In aggiunta ai requisiti di cui al punto 5.5.3.2, per gli esami svolti online da remoto devono essere rispettati almeno i seguenti requisiti:

- a) video/audio e sorveglianza attiva:
 - i. webcam frontale obbligatoria, attiva per tutta la sessione;
 - ii. audio attivo (per rilevare voci o rumori sospetti);
 - iii. registrazione video continua e non disattivabile, anche dello schermo dell'esame (opzionale);
 - iv. la piattaforma implementa un sistema di proctoring che consenta al proctor di monitorare in tempo reale le sessioni d'esame attive e gli utenti partecipanti. L'attivazione del monitoraggio deve essere resa nota all'utente prima dell'avvio della sessione d'esame. Gli utenti devono essere chiaramente e preventivamente informati circa l'attivazione delle funzionalità di monitoraggio della sessione d'esame;
- b) controllo dell'ambiente digitale (browser):
 - i. disabilitazione delle funzioni di stampa, copia/incolla, screenshot e comandi tastiera non autorizzati;
 - ii. inibizione delle funzioni di cambio finestra o applicazioni diverse da quella su cui si svolge la prova d'esame;
 - iii. monitoraggio attivo dello schermo tramite condivisione in tempo reale (live sharing) con il proctor e/o registrazione della sessione d'esame.

Le misure di cui ai punti i) e ii) devono essere implementate mediante soluzioni che si limitino a inibire le funzionalità non consentite, senza tenere traccia delle operazioni effettuate dal candidato (quali attività su internet, applicazioni utilizzate, tasti digitati sulla tastiera, movimenti o click del mouse);

NOTA: Non è ammessa la possibilità di richiedere l'installazione di software di controllo terzi o proprietari.

- c) anti-cheating e inibizione del comportamento fraudolento del candidato:
 - i. inibizione dell'uso improprio dei sistemi AI vocali o testuali;
 - ii. divieto di dispositivi hardware non autorizzati;

d) presidio del proctor:

- i. il proctor deve essere formato e qualificato e collegato in tempo reale;
- ii. il proctor deve intervenire via chat o via audio in caso di comportamenti sospetti;
- iii. il proctor deve sospendere o terminare la prova in tempo reale (possibilità di segnalazioni tracciate, con un massimo di 3 ammonimenti; al terzo ammonimento, avviene l'espulsione). Ogni decisione di sospensione o espulsione deve essere documentata;
- iv. il proctor deve mantenere la propria webcam attiva per l'intera durata della sessione d'esame, in modo da essere visibile ai candidati monitorati. La piattaforma deve conservare evidenza della presenza attiva del proctor nella sessione;
- v. ciascun proctor può monitorare simultaneamente un massimo di 50 candidati per sessione d'esame. Il rispetto di tale rapporto deve essere documentato e tracciato nel log della sessione;

5.5.3.4 REQUISITI PER ESAMI ONLINE DA REMOTO - LIVELLO AVANZATO OPZIONALE (SISTEMI AI)

In aggiunta ai requisiti di cui ai punti 5.5.3.2 e 5.5.3.3, l'OdC può implementare sistemi di monitoraggio basati sull'intelligenza artificiale a supporto del proctor. In tal caso, i seguenti requisiti devono essere rispettati:

a) condizioni per l'adozione di sistemi AI:

- i. l'OdC deve effettuare preventivamente una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'articolo 35 del Regolamento UE 2016/679. La DPIA deve essere documentata, aggiornata periodicamente e resa disponibile nell'ambito del sistema di gestione dell'OdC;
- ii. l'OdC deve classificare i sistemi AI adottati in conformità al Regolamento UE 2024/1689 (AI Act) e alla Legge 132/2025, individuando gli obblighi applicabili in relazione al livello di rischio;
- iii. l'OdC deve verificare se il sistema di IA adottato rientri tra i sistemi ad alto rischio ai sensi dell'Allegato III del Regolamento UE 2024/1689 (in particolare nell'ambito dell'istruzione e della valutazione) e, in tale caso, adempiere agli obblighi conseguenti;
- iv. l'OdC deve documentare nel proprio sistema di gestione la descrizione tecnica dei sistemi AI adottati, le relative finalità, le modalità di funzionamento e le procedure di revisione umana;

b) principio di supervisione umana

I sistemi AI devono operare esclusivamente come strumento di supporto al proctor e non possono in alcun caso sostituire il controllo umano. In particolare:

- i. tutte le decisioni relative alla sospensione, all'interruzione o all'annullamento della prova d'esame devono essere assunte tramite una conferma del proctor. Non è possibile rendere tali decisioni esclusivamente automatizzate;
- ii. ogni segnalazione generata dai sistemi automatizzati deve essere valutata e confermata da un intervento umano effettivo e documentato da parte del proctor prima di qualsiasi azione sul candidato;
- iii. il proctor deve avere la facoltà di disattendere le segnalazioni automatiche qualora le ritenga non fondate. Tale decisione deve essere motivata e tracciata nel log della sessione;

c) funzionalità ammesse

I sistemi AI possono includere le seguenti funzionalità, sempre nel rispetto delle condizioni di cui alle lettere a) e b):

- i. rilevazione automatizzata dell'assenza prolungata del candidato dall'inquadratura della webcam (verifica di presenza);
- ii. rilevazione automatizzata di voci o rumori ambientali anomali indicativi della presenza di soggetti terzi nell'ambiente d'esame;
- iii. registrazione video continua con possibilità di analisi automatizzata ex post (anche tramite AI), ai fini della verifica della regolarità della sessione;
- iv. sistemi avanzati di rilevazione dell'uso improprio di strumenti di intelligenza artificiale vocali o testuali da parte del candidato durante la prova;

NOTA: Non è consentito l'utilizzo di sistemi che comportino la raccolta e l'elaborazione automatizzata di dati relativi al comportamento del candidato (quali movimenti del corpo, movimenti oculari, frequenza dei click del mouse, operazioni compiute sulla tastiera, tentativi di accesso ad altre applicazioni, attività su Internet) al fine di elaborare indici di rischio o segnali di allerta relativi a possibili comportamenti fraudolenti.

d) informativa al candidato:

- i. l'OdC deve informare il candidato, prima dell'avvio della sessione d'esame, circa l'utilizzo di sistemi AI, specificando le tipologie di trattamento effettuate, le relative finalità e i diritti dell'interessato;
- ii. qualora il candidato non intenda sottoporsi al monitoraggio tramite sistemi AI, deve essergli garantita la possibilità di sostenere l'esame in modalità alternativa (livello minimo obbligatorio da remoto, ovvero in presenza presso sede secondaria dell'OdC), senza alcun effetto pregiudizievole sul processo certificativo;
- iii. l'informativa deve essere resa in forma chiara, concisa e facilmente accessibile, nel rispetto della legislazione vigente;

e) conservazione dei dati:

- i. i dati generati dai sistemi AI devono essere conservati per la durata di validità del certificato (2 anni), unitamente alla documentazione delle revisioni umane effettuate;
- ii. i dati generati dai sistemi AI non possono essere utilizzati per finalità diverse da quelle di prevenzione delle frodi e garanzia dell'integrità del processo certificativo;

f) rapporto proctor/candidati:

- i. in presenza di sistemi AI conformi ai requisiti del presente punto 5.5.3.4, il rapporto massimo tra proctor e candidati monitorati simultaneamente può essere elevato fino a 500 candidati per proctor, in considerazione del supporto fornito dai sistemi automatizzati nella rilevazione delle anomalie;
- ii. il proctor deve comunque essere presente alla propria postazione e deve essere visibile, mantenendo la propria webcam sempre attiva. Deve essere inoltre garantita la sua capacità di intervento diretto su qualsiasi candidato della sessione in tempo reale;
- iii. l'OdC deve documentare nel proprio sistema di gestione i criteri adottati per la determinazione del rapporto proctor/candidati.

5.5.3.5 REQUISITI PER ESAMI IN PRESENZA PRESSO SEDI SECONDARIE DELL'ODC

Lo svolgimento dell'esame può avvenire, in alternativa alla modalità da remoto, presso sedi secondarie dell'Organismo di Certificazione, sempre tramite la piattaforma digitale dell'OdC e nel rispetto di tutti i requisiti di cui al punto 5.5.3.2. Inoltre, si applicano i seguenti requisiti:

a) requisiti della sede:

- i. la sede deve essere formalmente individuata dall'OdC come sede secondaria, e riportata in visura camerale;
- ii. la sede deve disporre di un ambiente idoneo allo svolgimento delle prove d'esame, che garantisca condizioni adeguate di silenzio, illuminazione, separazione dai locali adibiti ad altre attività e assenza di interferenze esterne;
- iii. la sede deve disporre di postazioni informatiche dotate di connessione stabile, webcam e audio funzionanti, configurate per l'accesso alla piattaforma digitale dell'OdC;
- iv. le Pubbliche Amministrazioni censite nell'Indice delle Pubbliche Amministrazioni (IndicePA - indicepa.gov.it) possono ospitare sessioni di esame dell'OdC senza configurarsi come sedi secondarie dell'OdC stesso;
- v. non è ammesso l'utilizzo di sedi gestite da soggetti terzi, centri affiliati, test center o strutture convenzionate che operino con autonomia organizzativa, operativa, decisionale o commerciale rispetto all'OdC. La responsabilità della gestione della sede ricade integralmente sull'Organismo di Certificazione;

b) sorveglianza diretta:

- i. il proctor deve essere fisicamente presente nella sede d'esame per l'intera durata della sessione;
- ii. il proctor deve effettuare la verifica dell'ambiente fisico prima dell'avvio della sessione, accertando: l'assenza di materiali non autorizzati (appunti, dispositivi elettronici personali, libri, ecc.), l'assenza di dispositivi non consentiti, l'assenza di soggetti terzi non autorizzati nell'ambiente d'esame;
- iii. il proctor deve garantire il monitoraggio continuo dei candidati per l'intera durata della sessione d'esame e documentare eventuali anomalie nel log della sessione;
- iv. ciascun proctor non può sorvegliare simultaneamente più di 30 candidati. Il rispetto di tale rapporto deve essere documentato e tracciato nel log della sessione;

c) identificazione e riconoscimento:

- i. l'identificazione del candidato avviene tramite i sistemi digitali previsti ai punti 5.2 e 5.3 (SPID, CIE, eIDAS o KYC), anche in caso di svolgimento in presenza;
- ii. il riconoscimento del candidato è effettuato dal proctor fisicamente presente mediante confronto visivo diretto tra il candidato e il documento di identità in corso di validità;
- iii. l'avvenuto riconoscimento deve essere documentato e registrato nel log della sessione;

d) svolgimento dell'esame:

- i. l'esame deve essere svolto esclusivamente tramite la piattaforma digitale dell'OdC, con le medesime modalità, contenuti, tempistiche e criteri di valutazione previsti per la modalità da remoto;

- ii. non è consentito l'utilizzo di supporti cartacei o altri strumenti non integrati nella piattaforma dell'OdC;
- iii. la piattaforma deve garantire le medesime funzionalità di tracciamento, randomizzazione e generazione automatica dell'esito previste al punto 5.5.3.2.
- iv. l'OdC deve assicurare che le condizioni di svolgimento in presenza siano equivalenti, in termini di integrità e tracciabilità del processo, a quelle previste per la modalità da remoto.

Il seguente prospetto 3 chiarisce in quali fasi del processo di esame si applicano i requisiti tecnici sopra riportati.

Prospetto 3 – Rapporto tra caratteristiche tecniche e fasi del processo di esame

Fase del processo	Attività	Caratteristiche tecniche applicabili
Registrazione domanda di esame	Stabilire chi è la persona tramite la registrazione preliminare dei dati anagrafici	5.5.3.2 c), punto i
Verifica tecnica dei dispositivi (hardware)	Controllare che l'hardware sia conforme ai requisiti della piattaforma d'esame	5.5.3.2 b)
Ingresso in sala d'attesa e riconoscimento	Verificare che chi accede alla prova corrisponda alla persona identificata	5.5.3.2 c), punto ii 5.5.3.2 c), punto iii 5.5.3.3 d), punto i (da remoto) 5.5.3.5 b), punto i (in presenza)
Svolgimento dell'esame - da remoto (livello minimo)	Sostenimento della prova d'esame con monitoraggio umano in tempo reale	5.5.3.2 a) 5.5.3.3 a) 5.5.3.3 b) 5.5.3.3 c) 5.5.3.3 d) 5.5.3.2 e)
Svolgimento dell'esame - da remoto (sistemi AI)	Sostenimento della prova con monitoraggio AI a supporto del proctor umano	Requisiti del livello minimo + 5.5.3.4 (tutti i punti applicabili) 5.5.3.2
Svolgimento dell'esame - in presenza	Sostenimento della prova in presenza con sorveglianza diretta	5.5.3.2 a) 5.5.3.2 e) 5.5.3.5 tutti i punti
Conclusione dell'esame	Ottenimento dei risultati della prova	5.5.3.2 f)
Tutte le fasi	Caratteristiche applicabili a tutte le fasi del processo	5.5.3.2 a) punto ii 5.5.3.2 d) 5.5.3.2 g)

5.5.4 PROCESSO DI QUALIFICA DEGLI ESAMINATORI

Gli esaminatori e gli esperti tecnici coinvolti nel processo di certificazione devono essere qualificati secondo requisiti oggettivi e documentati, stabiliti all'interno del sistema qualità dell'organismo di certificazione.

La qualifica deve essere gestita mediante procedura strutturata che includa almeno i seguenti criteri minimi di accesso:

- titolo di studio almeno di livello EQF 5;
- esperienza professionale documentata di almeno 3 anni nel settore di riferimento di alfabetizzazione digitale;
- conoscenza documentata dei framework di riferimento (DigComp e/o DigCompEdu).

5.5.5 PROCESSO DI QUALIFICA DEI PROCTOR (SORVEGLIANTI)

I sorveglianti incaricati del presidio delle sessioni d'esame devono essere selezionati e qualificati attraverso criteri oggettivi, verificabili e coerenti con il sistema qualità dell'organismo di certificazione.

La qualifica deve essere gestita mediante procedura strutturata che includa almeno i seguenti criteri minimi:

- titolo di studio almeno di scuola secondaria di secondo grado;
- conoscenza documentata dei framework di riferimento (DigComp e/o DigCompEdu);
- conoscenza documentata della presente prassi di riferimento;
- conoscenza documentata della piattaforma utilizzata dall'Organismo di Certificazione;
- formazione documentata sulle procedure di sorveglianza, anti-frode e gestione della privacy;
- assenza di conflitti di interesse rispetto ai candidati della sessione d'esame;
- aggiornamento periodico documentato.

5.6 ELEMENTI PER IL MANTENIMENTO

Il certificato rilasciato dall'OdC non è soggetto a sorveglianze. Pertanto, non sono previsti mantenimenti.

5.7 ELEMENTI PER IL RINNOVO

La durata della certificazione deve essere pari a 2 anni, al termine dei quali deve essere ripetuto l'intero processo d'esame.

NOTA: Eventuali eccezioni possono essere previste per persone con bisogni speciali (**per esempio** comprovata impossibilità derivante da maternità/gravidanza, disabilità, DSA, gravi motivi di salute o altre cause di forza maggiore), attivando un processo compensativo.

5.8 RIFERIMENTO ALLA CERTIFICAZIONE E UTILIZZO DEL MARCHIO UNI

In aggiunta a quanto specificato dalla UNI CEI EN ISO/IEC 17024 si applica quanto segue:

- l'OdC deve concedere l'utilizzo del Marchio UNI alla persona certificata in conformità alla presente norma;
- l'OdC deve provvedere a sottoscrivere l'accordo di utilizzo del Marchio UNI in abbinamento al proprio marchio e deve disporre di regole che consentano alla persona di dichiarare la propria conformità ai requisiti della presente prassi;
- per rilasciare tale marchio alla persona, l'OdC deve disporre di regole per la concessione della licenza d'uso del proprio marchio di certificazione delle persone che ne preveda l'utilizzo combinato al Marchio UNI;
- l'utilizzo combinato del marchio dell'OdC e del Marchio UNI deve essere permesso a partire dalla data di emissione del certificato da parte dell'organismo.

NOTA: Il Marchio di conformità UNI ha lo scopo di attestare che i requisiti dell'attività di una persona, certificata da OdC accreditato per certificare la specifica figura, siano stabiliti da UNI tramite la pubblicazione di documenti tecnici UNI.

5.9 EMISSIONE DEI CERTIFICATI E RILASCIO OPEN BADGE DIGITALE

5.9.1 GENERALITÀ

Il presente punto definisce i requisiti per l'emissione dei certificati di competenza digitale e per il rilascio delle credenziali digitali verificabili, in conformità alla UNI CEI EN ISO/IEC 17024 e in coerenza con gli standard europei di interoperabilità. L'OdC deve garantire che i certificati emessi siano:

- conformi ai requisiti della presente prassi di riferimento;
- interoperabili coi sistemi europei di riconoscimento delle credenziali;
- verificabili in modo autonomo e indipendente dalla disponibilità dei sistemi dell'OdC;
- protetti contro contraffazione e manomissione mediante tecnologie crittografiche.

Ai fini della verificabilità autonoma e indipendente di cui sopra, il certificato deve incorporare un meccanismo di verifica crittografica (firma elettronica o sigillo elettronico, ovvero prova crittografica equivalente) che ne consenta la verifica di autenticità e integrità anche in assenza di connessione ai sistemi dell'OdC. La verifica online di cui al punto 5.9.2 (QR code o URI) costituisce modalità di riscontro complementare e non sostitutiva.

NOTA: Un esempio di certificato e un esempio di Open Badge sono riportati in Appendice B.

5.9.2 CONTENUTO DEL CERTIFICATO

In conformità alla UNI CEI EN ISO/IEC 17024, il certificato deve riportare almeno le seguenti informazioni:

- a) nome e cognome della persona certificata;
- b) codice fiscale;
- c) ID univoco del certificato con codice alfanumerico non riutilizzabile;
- d) data di prima emissione del certificato;
- e) data di emissione corrente del certificato;
- f) data di scadenza del certificato;
- g) denominazione e dati identificativi dell'Organismo di Certificazione;
- h) riferimento allo schema di certificazione applicato, con indicazione del framework di riferimento (DigComp o DigCompEdu) e della versione o della data di emissione dello schema;
- i) riferimento alla presente UNI/PdR;
- j) marchio di Accredia;
- k) riferimento al Marchio UNI, ove applicabile;
- l) un QR code o URI che consenta la verifica online del certificato (anche verso il registro pubblico di Accredia, laddove applicabile);

m) campo di applicazione della certificazione comprensivo di:

- livello di padronanza conseguito (per esempio “livello intermedio” per DigComp, o “livello B2” per DigCompEdu), ovvero la media totale del livello raggiunto;
- tabella con aree di competenza e livello raggiunto per ciascuna area;

n) firma del rappresentante legale (o della persona delegata) dell’Organismo di Certificazione.

5.9.3 OPEN BADGE DIGITALE (OPZIONALE)

5.9.3.1 GENERALITÀ

Laddove si decida di utilizzare un Open Badge Digitale, l’OdC deve effettuarne il rilascio, contestualmente al certificato e in conformità alla specifica *Open Badges 2.0, 2.1, 3.0* pubblicata da 1EdTech (ex IMS Global Learning Consortium)¹.

L’Open Badge Digitale può essere rilasciato solo qualora sia associato a un certificato di conformità emesso dall’OdC. L’Open Badge deve risultare univocamente collegato al certificato di riferimento e deve consentire la verifica dell’autenticità e della validità della certificazione tramite identificativo univoco e/o URL di verifica.

L’Open Badge deve essere strutturato come *Verifiable Credential* conforme al *W3C Verifiable Credentials Data Model v2.0* e successivi, garantendo:

- verificabilità crittografica indipendente dall’OdC;
- portabilità in digital wallet conformi agli standard;
- interoperabilità con piattaforme di terze parti.

5.9.3.2 STRUTTURA DELL’OPEN BADGE

L’Open Badge deve contenere almeno i seguenti elementi:

Dati dell’*Achievement* (Risultato conseguito):

- nome della certificazione (per esempio “Certificazione DigComp 3.0 - Livello Intermedio”);
- descrizione della competenza certificata;
- criteri di conseguimento con riferimento al framework applicato;
- livello di padronanza conseguito;
- il Marchio Accredia;
- il riferimento alla presente UNI/PdR.

Dati dell’*Issuer* (Emittente):

- denominazione dell’OdC;
- identificativo univoco dell’OdC (DID - Decentralized Identifier o URI);
- URL del profilo pubblico dell’OdC;
- numero di accreditamento Accredia (facoltativo).

1) https://site.imsglobal.org/certifications?refinementList%5Bstandards_lvlx%5D%5B0%5D=Open%20Badges

Dati del *Recipient* (Destinatario):

- identificativo del destinatario (DID o identificativo verificabile).

Non deve essere utilizzato l'indirizzo e-mail come unico identificativo per ragioni di privacy e persistenza.

Dati della *Credential* (Credenziale):

- identificativo univoco della credenziale;
- data di emissione (issuanceDate);
- data di scadenza (expirationDate);
- prova crittografica (proof) conforme a Data Integrity EdDSA o ECDSA Cryptosuites (opzionale).

5.9.3.3 FORMATO TECNICO

L'Open Badge deve essere rilasciato in formato JSON-LD, con possibilità di incorporamento (baking) in file immagine PNG o SVG per facilitarne la condivisione sui social media e nelle piattaforme professionali. L'OdC deve rendere disponibile:

- il file JSON-LD della credenziale verificabile;
- l'immagine del badge con metadati incorporati;
- un URL di verifica accessibile pubblicamente.

5.9.4 INTEROPERABILITÀ (OPZIONALE)

5.9.4.1 ALLINEAMENTO ALLO EUROPEAN LEARNING MODEL (ELM)

L'OdC può garantire che le credenziali emesse siano compatibili con l'European Learning Model (ELM) sviluppato dalla Commissione Europea nell'ambito dell'Europass Digital Credentials Infrastructure (EDCI).

A tal fine, il certificato digitale può includere i seguenti elementi ELM:

- a) **LearningAchievement**: descrizione strutturata del risultato di apprendimento conseguito, con riferimento alle competenze del framework DigComp o DigCompEdu.
- b) **LearningAssessment**: informazioni sulla valutazione sostenuta, inclusi metodo, data e risultato.
- c) **AwardingBody**: informazioni sull'OdC quale organismo che rilascia la certificazione.
- d) **Accreditation**: riferimento all'accREDITamento Accredia dell'OdC.

5.9.4.2 COMPATIBILITÀ EUROPASS

L'OdC può consentire l'esportazione del certificato in formato compatibile con il portafoglio Europass, permettendo alla persona certificata di:

- importare la credenziale nel proprio profilo Europass;
- condividere la credenziale con datori di lavoro e istituzioni in tutta l'Unione Europea;
- beneficiare della verifica automatica dell'autenticità tramite i servizi Europass.

6 REQUISITI SUPPLEMENTARI PER PERSONE CON BISOGNI SPECIALI

Il sistema di certificazione deve prevedere misure di accesso e compensative specifiche per candidati che dichiarino di essere in condizioni di svantaggio o fragilità, ad esempio impossibilità derivante da maternità/gravidanza, disabilità, DSA, gravi motivi di salute o altre cause di forza maggiore.

La dichiarazione deve essere conforme all'articolo 46 del DPR 445/2000 (e successive modifiche e integrazioni). Tali misure possono essere attivate esclusivamente su richiesta del candidato, attraverso la piattaforma digitale, in fase di presentazione della domanda.

Le misure compensative possono includere, ad esempio:

- estensione del tempo di svolgimento della prova;
- utilizzo di strumenti di supporto (per esempio lettori vocali, ingranditori);
- svolgimento dell'esame in date o modalità alternative, nel rispetto dei criteri di imparzialità e tracciabilità;
- presenza di un facilitatore o tutor, ove necessario.

APPENDICE A (INFORMATIVA)

ESEMPI DI COMPORTAMENTI NON RACCOMANDATI

A.1. GENERALITÀ

La presente Appendice descrive i comportamenti non conformi, che non dovrebbero essere adoperati nell'applicazione del presente documento.

A.2. COMPORTAMENTI NON RACCOMANDATI GENERALI

Le seguenti azioni non dovrebbero essere effettuate lungo tutto l'arco del processo di valutazione della conformità, di cui al punto 5 della presente prassi:

- l'identificazione del/la candidato/a non dovrebbe essere effettuata attraverso modalità non digitali e non tracciabili;
- non dovrebbero essere utilizzate piattaforme non conformi ai requisiti di tracciabilità e conservazione digitale del processo;
- non dovrebbero essere utilizzate modalità cartacee, supporti fisici o ambienti non tracciabili.

A.3. COMPORTAMENTI NON RACCOMANDATI INERENTI ALL'ACCESSO ALLA CERTIFICAZIONE (5.2)

Le seguenti azioni non dovrebbero essere effettuate in fase di accesso alla certificazione:

- non dovrebbero essere imposti percorsi formativi obbligatori come conditio sine qua non per l'accesso alla certificazione;
- il/la candidato/a non dovrebbe essere vincolato/a all'acquisto di servizi aggiuntivi (per esempio formazione, materiali didattici, tutoraggi) come prerequisito per l'ammissione all'esame.

A.4. COMPORTAMENTI NON RACCOMANDATI INERENTI ALLA MODALITÀ DI IDENTIFICAZIONE (5.3)

Le seguenti azioni non dovrebbero essere effettuate in fase di identificazione del/la candidato/a:

- non dovrebbero essere accettati documenti cartacei, scansioni o fotografie inviate via e-mail come forma di identificazione;
- non dovrebbero essere utilizzate modalità di riconoscimento non integrate nella piattaforma o prive di tracciabilità;
- l'identificazione non dovrebbe essere delegata a soggetti terzi non autorizzati e non qualificati dall'Organismo di Certificazione.

A.5. COMPORTAMENTI NON RACCOMANDATI INERENTI AI METODI DI VALUTAZIONE APPLICABILI E ALLO SVOLGIMENTO DELLE PROVE (5.5.2)

Le seguenti azioni inerenti ai metodi di valutazione applicabili non dovrebbero essere effettuate:

- non dovrebbero essere somministrate prove differenti da quelle previste dalla presente prassi;
- non dovrebbero essere somministrati esami in assenza di piattaforma online validata dall'OdC;
- non dovrebbero essere modificati i criteri di valutazione, rispetto a quanto previsto dalla presente prassi di riferimento.

Le seguenti azioni non dovrebbero essere effettuate in fase di svolgimento delle prove:

- non dovrebbe essere ammessa alcuna forma di assistenza esterna al candidato durante la prova, fatti salvi i casi in cui siano previste misure di supporto documentate a favore di candidati con esigenze personali, familiari, sanitarie o di altra natura, che rendano necessario un adattamento del processo valutativo (vedere anche punto 6 della presente prassi);
- non dovrebbero essere imposte soglie arbitrarie o non documentate;
- non dovrebbero essere certificati livelli diversi da quelli conseguiti durante la prova d'esame;
- non dovrebbero essere previsti percorsi di esame frazionati o basati su integrazione di certificazioni pregresse.

A.6. COMPORTAMENTI NON RACCOMANDATI INERENTI AL PROCESSO DI QUALIFICA DEGLI ESAMINATORI/ESPERTI TECNICI (5.5.4)

Le seguenti azioni non dovrebbero essere effettuate in fase qualifica degli esaminatori:

- non dovrebbero essere designati esaminatori/esperti tecnici che non soddisfano i criteri riportati al punto 5.5.4;
- non dovrebbero essere affidati incarichi a soggetti privi di formazione specifica o aggiornamento periodico;
- non dovrebbero essere consentiti conflitti di interesse tra esaminatore/esperto tecnico ed esaminato (inclusi legami familiari, relazioni lavorative dirette o indirette);
- non dovrebbe essere fatto riferimento ad esaminatori/esperti tecnici non nominativamente identificabili e non registrati nel sistema qualità digitale.

A.7. COMPORTAMENTI NON RACCOMANDATI INERENTI AL PROCESSO DI QUALIFICA DEI PROCTOR (5.5.5)

Le seguenti azioni non dovrebbero essere effettuate in fase qualifica dei proctor:

- non dovrebbero essere nominati come sorveglianti soggetti privi di formazione o non identificabili digitalmente;
- non dovrebbe essere fatto ricorso a modalità di vigilanza non tracciabili, offline o basate su strumenti cartacei;
- non dovrebbe essere consentita la presenza di sorveglianti che operino senza registrazione ufficiale nella sessione o senza tracciamento delle attività svolte;
- non dovrebbero essere coinvolti sorveglianti che abbiano interessi diretti o indiretti nei confronti dell'esaminando.

A.8. COMPORTAMENTI NON RACCOMANDATI IN CASO DI PERSONE CON BISOGNI SPECIALI (6)

Le seguenti azioni non dovrebbero essere effettuate in caso di presenza di persone con bisogni speciali:

- non dovrebbe essere richiesta documentazione non pertinente, eccessiva o discriminatoria rispetto alla condizione dichiarata;

- non dovrebbe essere negato l'accesso alla certificazione per il solo fatto della presenza di una fragilità documentata;
- non dovrebbero essere erogate misure non tracciate o non coerenti con quanto previsto nello schema;
- non dovrebbero essere utilizzati canali non digitali per la presentazione o la gestione di tali richieste.

APPENDICE B (INFORMATIVA)

ESEMPI DI CERTIFICATO E OPEN BADGE

Le figure riportate nella presente appendice sono ad esclusivo fine esemplificativo e riportano tutti gli elementi richiesti nei punti 5.9.2 (certificato) e 5.9.3 (Open Badge digitale)

Figura B.1 – Esempio di certificato DigComp

MARCHIO CAB

SI CERTIFICA CHE
in conformità alla UNI/PdR 193:2026
e al framework europeo
Digital Competence of Educators - DigCompEdu

Nome COGNOME

POSSIEDE LE COMPETENZE
in accordo allo schema

DigCompEdu

ESPERTO B2
Livello di padronanza generale

con i seguenti livelli di padronanza per
ciascuna area di competenza

AREA di COMPETENZA	LIVELLO di PADRONANZA	
Coinvolgimento e valorizzazione professionale	NOVIZIO	A1
Risorse digitali	ESPLORATORE	A2
Pratiche di insegnamento e apprendimento	SPERIMENTATORE	B1
Valutazione dell'apprendimento	ESPERTO	B2
Valorizzazione delle potenzialità degli studenti	LEADER	C1
Favorire lo sviluppo delle competenze digitali degli studenti	PIONIERE	C2

Il presente certificato è composto da una pagina

**MARCHIO
ACCREDIA
MARCHIO UNI**

CODICE FISCALE
XXXXXXXXXXXXXXXXXX
NATO/A a
CITTA' - XX/XX/1989
ID CERTIFICATO
#XX-XXX-XXX

DATA di PRIMA EMISSIONE
12/02/2020
DATA di EMISSIONE CORRENTE
20/07/2024
DATA di SCADENZA
19/07/2028

N. CERTIFICATO
A-XXXXXXXXXX



VERIFICA LA TUA
CERTIFICAZIONE

firma

Amministratore Delegato
XXXXX srl
Via XXXXXXXXX, 1
CAP CITTA'

Figura B.2 – Esempio di certificato DigCompEdu

MARCHIO CAB

SI CERTIFICA CHE

in conformità alla UNI/PdR 193:2026 e
al framework europeo
Digital Competence framework for
Citizen DigComp

Nome COGNOME

POSSIEDE LE COMPETENZE
in accordo allo schema

DigComp 2.2

AVANZATO
Livello di padronanza generale di competenza

con i seguenti livelli di padronanza per
ciascuna area di competenza

AREA di COMPETENZA	LIVELLO di PADRONANZA
Alfabetizzazione su informazione e dati	ALTAMENTE AVANZATO
Comunicazione e collaborazione	AVANZATO
Creazione contenuti digitali	INTERMEDIO
Sicurezza	AVANZATO
Risolvere problemi	BASE

Il presente certificato è composto da una pagina

**MARCHIO
ACCREDIA
MARCHIO UNI**

CODICE FISCALE
XXXXXXXXXXXXXXXXXX
NATO/A a
CITTA' - XX/XX/1989
ID CERTIFICATO
#XX-XXX-XXX

N. CERTIFICATO
A-XXXXXXXXXX



VERIFICA LA TUA
CERTIFICAZIONE

firma

Amministratore Delegato
XXXXX srl
Via XXXXXXXXX, 1
CAP CITTA'

Figura B.3 – Esempio di Open Badge digitale



BIBLIOGRAFIA

- [1] CEN Guide 14:2010, Common policy guidance for addressing standardisation on qualification of professions and personnel
- [2] CENTENO, C., COSGROVE, J., CACHIA, R., MORA, T., DI LEGGE, A., VIVARELLI, S., BULIAN, G., MOYES PRELLEZO, N., PIÑA DE SANTISTEBAN, P., SCHULZ, C., HÜSING, T., CUARTAS-ACOSTA, A. and TROIA, S., European Digital Skills Certificate (EDSC) Feasibility Study, Publications Office of the European Union, Luxembourg, 2024, doi:10.2760/958195, JRC138344.
- [3] DigComp 3.0: European Digital Competence Framework - Fifth Edition, Cosgrove, J., Cachia R., Publications Office of the European Union, Luxembourg, 2025
- [4] European Framework for the Digital Competence of Educators: DigCompEdu, Redecker C., Punie Y., Publications Office of the European Union, Luxembourg, 2017
- [5] DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, Vuorikari R., Kluzer S., Punie Y., Publications Office of the European Union, Luxembourg, 2022
- [6] Regolamento UE n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
- [7] Decreto Legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale
- [8] Europass Digital Credentials, European Union
<https://europass.europa.eu/it/european-digital-credentials>
- [9] Micro-Credentials and European Digital Credentials for Learning, European Union
<https://europass.europa.eu/en/news/micro-credentials-and-european-digital-credentials-learning>
- [10] A European approach to micro-credentials, European Commission, 2021
<https://education.ec.europa.eu/sites/default/files/2022-01/micro-credentials%20brochure%20updated.pdf>
- [11] Microcredenziali per l'apprendimento permanente e l'occupabilità: raccomandazioni, European Union
<https://eur-lex.europa.eu/IT/legal-content/summary/micro-credentials-for-lifelong-learning-and-employability-recommendations.html>
- [12] FAQ del Garante per la protezione dei dati personali "Sistemi di supervisione per la regolarità di prove d'esame e corsi a distanza", pubblicate il 15 aprile 2026
<https://www.garanteprivacy.it/temi/istruzione-e-formazione/esami-e-corsi-a-distanza>
- [13] Provvedimento Garante n. 35/2026, Cassazione 12967/2024, Tribunale di Milano 8872/2026



UNI Ente Italiano di Normazione
Membro italiano ISO e CEN

Via Sannio, 2 - 20137 Milano
Via del Collegio Capranica, 4 - 00186 Roma

www.uni.com



normeUNI



@normeUNI



normeUNI

Membro italiano ISO e CEN
www.uni.com
www.youtube.com/normeuni
www.x.com/normeuni
www.linkedin.com/company/normeuni