

UNI/PdR xx: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)
Sommario	La presente 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: a) i livelli di padronanza per le aree di competenza; b) le metodologie e gli ambiti di valutazione; c) gli indicatori di prestazione; d) i requisiti di processo per gli organismi che operano nell'ambito della valutazione della conformità.
Data	2025-xx-xx

Avvertenza

Il presente documento è un progetto di Prassi di Riferimento (UNI/PdR) sottoposta alla fase di consultazione, da utilizzare solo ed esclusivamente per fini informativi e per la formulazione di commenti.

Il processo di elaborazione delle Prassi di Riferimento prevede che i progetti vengano sottoposti alla consultazione sul sito web UNI per raccogliere i commenti del mercato: la UNI/PdR definitiva potrebbe quindi presentare differenze rispetto al documento messo in consultazione.

Questo documento perde qualsiasi valore al termine della consultazione, cioè il: 24 marzo 2026

UNI non è responsabile delle conseguenze che possono derivare dall'uso improprio del testo dei progetti di Prassi di Riferimento in consultazione.

PREMESSA

La presente prassi di riferimento UNI/PdR xx: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 "TITOLO DEL TAVOLO" condotto da UNI, costituito dai seguenti esperti:

Nome Cognome 1 – Project Leader (organizzazione xyz)

Nome Cognome 2 (organizzazione yz)

Nome Cognome 3 (organizzazione xyz)

Nome Cognome 4 (organizzazione y)

Nome Cognome 5 (organizzazione xz)

Nome Cognome 6 (organizzazione z)

La presente prassi di riferimento è stata ratificata dal Presidente dell'UNI il xx xxxx 2025.

Le prassi di riferimento, adottate esclusivamente in ambito nazionale, rientrano fra i "prodotti della normazione europea", come previsti dal Regolamento UE n.1025/2012, e sono documenti che introducono prescrizioni tecniche, elaborati sulla base di un rapido processo ristretto ai soli autori, sotto la conduzione operativa di UNI.

Le prassi di riferimento sono disponibili per un periodo non superiore a 5 anni, tempo massimo dalla loro pubblicazione entro il quale possono essere trasformate in un documento normativo (UNI, UNI/TS, UNI/TR) oppure devono essere ritirate.

Chiunque ritenesse, a seguito dell'applicazione della presente prassi di riferimento, di poter fornire suggerimenti per un suo miglioramento è pregato di inviare i propri contributi all'UNI, Ente Italiano di Normazione, che li terrà in considerazione.

SOMMARIO	pag
INTRODUZIONE	4
1 SCOPO E CAMPO DI APPLICAZIONE	6
2 RIFERIMENTI NORMATIVI E LEGISLATIVI.....	6
3 TERMINI E DEFINIZIONI	6
4 PRINCIPIO	10
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
5.5.3 Caratteristiche tecniche obbligatorie	14
5.5.4 Processo di qualifica degli esaminatori	16
5.5.5 Processo di qualifica dei proctor (sorveglianti)	17
5.6 Elementi per il mantenimento	17
5.7 Elementi per il rinnovo	17
5.8 Riferimento alla certificazione e utilizzo del Marchio UNI	17
5.9 Emissione dei certificati e rilascio Open Badge Digitale	18
5.9.1 Generalità	18
5.9.2 Contenuto del certificato	18
5.9.3 Open Badge Digitale	19
5.9.4 Interoperabilità (opzionale).....	20
6 Requisiti supplementari per persone con bisogni speciali.....	20
A.1. Generalità	22
A.2. Comportamenti non conformi generali	22
A.3. Comportamenti non conformi inerenti all'accesso alla certificazione (5.2).....	22

A.4. Comportamenti non conformi inerenti alla modalità di identificazione (5.3)	22
A.5. Comportamenti non conformi inerenti ai metodi di valutazione applicabili e allo svolgimento delle prove (5.5.2)	22
A.6. Comportamenti non conformi inerenti al processo di qualifica degli esaminatori/esperti tecnici (5.5.4)	23
A.7. Comportamenti non conformi inerenti al processo di qualifica dei proctor (5.5.5)	23
A.8. Comportamenti non conformi in caso di persone con bisogni speciali (6)	23
APPENDICE B	25
BIBLIOGRAFIA	28

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 D.Lgs. 13/2013, né un'attestazione ai sensi della L. 4/2013, ma rappresentano una base per la certificazione volontaria di parte terza secondo 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 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 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 D.M. 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 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 (es. 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 presente 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:

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

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 17024:2012, *Valutazione della conformità - Requisiti generali per organismi che eseguono la certificazione di persone*

ISO CASCO Guidance of ISO/IEC 17024

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 e del QNQ 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, Art. 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, Art. 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, Art. 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 ed assicurare la propria imparzialità nei confronti di ogni candidato.

NOTA il centro d'esami non emette certificazioni, come previsto dalla ISO/IEC 17024.

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 (3.8) di un/a candidato/a mediante uno o più mezzi quali prove scritte, orali, pratiche ed osservazione diretta.

[FONTE: UNI CEI EN ISO/IEC 17024:2012, 3.9 – 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.

NOTA: Ai fini di questa PdR l'esaminatore potrebbe essere figura non presente in sede di esame, qualora il materiale d'esame sia stato preventivamente validato e approvato dall'OdC.

[FONTE: UNI CEI EN ISO/IEC 17024:2012, 3.10 – con modifiche ad ulteriore dettaglio]

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 (3.7), 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 ad un esame (3.9), ma che non valuta la competenza (3.7) del/della candidato/a.

[FONTE: UNI CEI EN ISO/IEC 17024:2012, 3.11]

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 ad 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 finalizzato a prevenire frodi e garantire l'autenticità della partecipazione agli esami, condotto nel rispetto della normativa sulla privacy e sulla protezione dei dati personali.

NOTA Alcuni esempi di sistemi KYC sono: Stripe Identity, In Persona, ecc.

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 (notazione KSA) del framework stesso; certifica che il titolare ha acquisito concretamente quella competenza, tramite un percorso formativo breve e verificabile.

NOTA 1 Nel contesto della presente prassi, le certificazioni relative a singoli livelli di padronanza o aree di competenza dei framework DigComp e DigCompEdu non costituiscono micro-credenziali, in quanto l'esame deve essere sostenuto nella sua interezza (vedi 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 learning outcome KSA – competence statements

scenario di suddivisione della singola competenza, basata anche sui descrittori di Conoscenza (*Knowledge*), Abilità (*Skill*) e Attitudine (*Attitude*).

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,
- 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.

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.

La piattaforma 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 (es. 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 ISO/IEC 17024.

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);
- Consenso informato al trattamento dei dati personali (GDPR);
- 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). Vedere anche punto 6.

La conferma dell'invio della domanda e l'ammissione al processo di certificazione devono essere 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 al punto 9.1.3 della UNI CEI EN ISO/IEC 17024:2012 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 cloud, 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 il riconoscimento certo del soggetto.

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, anche al fine di garantire la trasparenza e la validità del processo certificativo.

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, con autorizzazione dei genitori.

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 sul portale dell'OdC, senza alcun supporto cartaceo, rivolto a profili utente ("USER").

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 01 – 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
	2	A2
Intermedio	3	B1
	4	B2
Avanzato	5	C1
	6	
Altamente avanzato	7	C2
	8	

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 pag. 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: per ogni domanda devono essere proposte almeno 4 risposte delle quali 1 sola è corretta (da escludere quelle del tipo "vero/falso"). Ciascuno step è composto da uno scenario learning outcome KSA – competence statements, con almeno 1 domanda per ogni competenza (i.e. 21 per DigComp e 22 DigCompEdu), per ciascuno dei livelli (i.e. 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 1 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.

NOTA 2 Lo scenario KSA learning outcome KSA – competence statements ha la funzione di rilevare tutti e tre i descrittori della singola competenza tramite un'unica domanda, come esemplificato nell'Annex 2 del DigComp 3.0.

3. L'esame DigComp è strutturato in step progressivi. Ciascuno step ha una durata massima di 60 minuti, calcolata considerando un tempo medio di 3 minuti per domanda, e una durata

minima non inferiore a 10 minuti. Per ciascuno step d'esame sono definite due soglie distinte: una soglia minima di conferma di validità dello step, fissata al 50% di risposte corrette, necessaria affinché lo step sia considerato utilmente svolto; una soglia di avanzamento, fissata al 75% di risposte corrette, che consente l'accesso allo step successivo. Il mancato raggiungimento della soglia di avanzamento non comporta penalizzazioni sul livello di competenza già certificato. In tal caso, il processo di valutazione si interrompe e il livello certificato corrisponde all'ultimo step validamente superato. A titolo esemplificativo, qualora il candidato non raggiunga la soglia minima prevista nello Step 1, il livello certificato rimane Base (DigComp).

4. L'esame DigCompEdu è strutturato in step progressivi. Ciascuno step ha una durata massima di 120 minuti, calcolata considerando un tempo medio di 3 minuti per domanda, e una durata minima non inferiore a 20 minuti. Per ciascuno step d'esame sono definite due soglie distinte: una soglia minima di conferma di validità dello step, fissata al 25% di risposte corrette, necessaria affinché lo step sia considerato utilmente svolto; una soglia di avanzamento, fissata al 75% di risposte corrette, che consente l'accesso allo step successivo. Il mancato raggiungimento della soglia di avanzamento non comporta penalizzazioni sul livello di competenza già certificato. In tal caso, il processo di valutazione si interrompe e il livello certificato corrisponde all'ultimo step validamente superato. A titolo esemplificativo, qualora il candidato non raggiunga la soglia minima prevista nello Step 1, il livello certificato rimane A1 (DigCompEdu).

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.

Non è possibile ricondurre il superamento di un singolo scenario all'ottenimento di micro-credenziali.

5.5.3 Caratteristiche tecniche obbligatorie

I seguenti requisiti inerenti alle caratteristiche tecniche devono essere rispettati:

- a) 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 (*hardware*) del discente prima dell'accesso alla sala d'attesa:
 - 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 identificazione:
 - i. autenticazione tramite SPID/CIE/IT Wallet o KYC biometrico
 - ii. identificazione candidato da proctor (umano) con matching facciale in tempo reale (via webcam + documento)
 - iii. conferma di assenza di conflitto di interessi tra proctor (se umano) e singolo candidato
- d) video/audio e sorveglianza attiva:

- i. Webcam frontale obbligatoria (HD 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 consente al proctor di monitorare in tempo reale le sessioni d'esame attive e gli utenti partecipanti.
L'attivazione del monitoraggio è 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
- e) controllo dell'ambiente digitale (browser):
- i. Browser (blocco funzioni stampa, copia/incolla, screenshot, comandi tastiera)
 - ii. Browser (impedire cambio finestra)
 - iii. Monitoraggio attivo dello schermo (activity recording e/o live sharing)
- NOTA: non è ammessa la possibilità di richiedere l'installazione di software di controllo terzi o proprietari.
- f) sistema anti-cheating/controllo comportamento candidato:
- i. Agenti AI per real-time control (per funzione di controllo durante l'esame)
 - ii. Blocco e detenzione dei sistemi AI vocali o testuali
 - iii. Sistemi di alert automatici su movimenti oculari sospetti, assenza del candidato, rumori esterni, tentativi di manipolazione del browser
 - iv. Divieto di occhiali con telecamera integrata
- g) presidio del proctor:
- i. Proctor formato e qualificato collegato in tempo reale
 - ii. Intervenire via chat o audio in caso di sospetti
 - iii. Sospendere o terminare la prova in tempo reale (possibilità di segnalazioni tracciate, con un massimo di 3 ammonimenti, al terzo ammonimento, avviene l'espulsione)
- h) logging e tracciabilità:
- i. Log automatico di:
 - Accessi (modalità connessione e identificazione)
 - Eventi sospetti
 - Interventi del proctor
 - Tentativi di cheating
 - ii. Conservazione dei log per almeno 2 anni
 - iii. Conservazione dei video (se registrati) almeno fino a delibera o per 30 giorni
 - iv. Collegamento tra:
 - Riconoscimento dell'identità verificata dell'utente
 - Proctor della sessione d'esame
 - Sessione d'esame
 - Risultato conseguito
- i) misure di emergenza e segnalazione:
- i. Pulsante (es. 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

- j) il risultato finale non granulare deve essere visibile al candidato alla fine dell'esame
- k) la piattaforma deve essere validata dall'OdC

Il seguente prospetto 02 chiarisce in quali fasi del processo di esame si applicano i requisiti tecnici sopra riportati.

Prospetto 02 – 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	c) i;
Verifica tecnica dei dispositivi (hardware)	Controllare che l'hardware sia conforme ai requisiti della piattaforma d'esame	b) (tutti i punti)
Ingresso in sala d'attesa e accettazione alla prova d'esame	Verificare che chi accede alla prova corrisponde alla persona precedentemente identificata	c) ii; c) iii; g) i;
Svolgimento dell'esame	Sostenimento della prova d'esame e relativo monitoraggio	a) i; a) iii; d) (tutti i punti); e) (tutti i punti); f) (tutti i punti); g) (tutti i punti); i) (tutti i punti);
Conclusione dell'esame	Ottenimento dei risultati della prova	j);
Tutte le fasi	Caratteristiche applicabili a tutte le fasi del processo	a) ii; h) (tutti i punti); k;

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 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 e di seguito elencate.

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

Prospetto 03 — Elementi per il rinnovo

Durata della certificazione:	2 anni
Modalità di rinnovo:	Ripetizione dell'intero processo di esame

NOTA Eventuali eccezioni possono essere previste per persone con bisogni speciali (es. 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 al punto 4.1 “Aspetti legali” della 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 norma;
- 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 ai punti 9.4.8 e 9.4.9 della UNI 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.

NOTA Un esempio di certificato e un esempio di Open Badge sono riportati in Appendice C

5.9.2 Contenuto del certificato

In conformità al punto 9.4.8 della UNI EN ISO/IEC 17024, il certificato deve riportare almeno le seguenti informazioni:

- Nome e cognome della persona certificata;
- Codice Fiscale;
- ID univoco del certificato con codice alfanumerico non riutilizzabile;
- Data di prima emissione del certificato;
- Data di emissione corrente del certificato;
- Data di scadenza del certificato;
- Denominazione e dati identificativi dell'Organismo di Certificazione;
- 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;
- Riferimento alla presente UNI/PdR;
- Logo di Accredia
- Riferimento al Marchio UNI, ove applicabile;
- Un QR code o URI che consenta la verifica online del certificato (anche verso il registro pubblico di Accredia, laddove applicabile);
- Campo di applicazione della certificazione comprensivo di:
 - Livello di padronanza conseguito (es. "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;
- Firma del rappresentante legale (o della persona delegata) dell'Organismo di Certificazione.

5.9.3 Open Badge Digitale

5.9.3.1 Generalità

Laddove si decida di utilizzare un Open Badge Digitale, l'OdC deve effettuare 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 (es. "Certificazione DigComp 3.0 - Livello Intermedio");
- descrizione della competenza certificata;
- criteri di conseguimento con riferimento al framework applicato;
- livello di padronanza conseguito;
- il logo Accredia;
- 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).

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.

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

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'art. 46 del DPR 445/2000 (e smi). Tali misure possono essere attivate esclusivamente su richiesta del candidato, attraverso la piattaforma cloud, 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 (es. 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.

BOZZA PER CONSULTAZIONE

APPENDICE A (informativa)

ESEMPI DI COMPORTAMENTI NON CONFORMI

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 conformi 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 o 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 conformi 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 (es. formazione, materiali didattici, tutoraggi) come prerequisito per l'ammissione all'esame.

A.4. Comportamenti non conformi 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 conformi 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 dematerializzata 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 conformi 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 conformi 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 conformi 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.

BOZZA PER CONSULTAZIONE

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).

MARCHIO CAB

SI CERTIFICA CHE

in conformità alla UNI/PdR XXX: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 DigComp

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

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'

Il presente certificato è composto da una pagina

Figura B.1 – Esempio di certificato DigComp

© UNI

25

MARCHIO CAB

SI CERTIFICA CHE
in conformità alla UNI/PdR XXX: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 ottenuto

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



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>