



14 giugno 2024

Consultazione sulla scelta della tecnologia concernente l'infrastruttura di fiducia e l'Id-e

Sintesi dei pareri

Indice

1	Situazione iniziale	4
2	Risultati	5
2.1	Qual è lo scenario preferito e perché?	5
2.2	Entrambi gli scenari soddisfano le aspettative?	7
2.3	In cosa consistono i rischi principali?	8
2.4	Quali sono i limiti da non oltrepassare?	9
2.5	Altre osservazioni	9
3	Osservazioni finali	10
4	Allegati	11
4.1	Membri del Technical Advisory Circle (TAC).....	11
4.2	Elenco dei partecipanti alla consultazione	11
4.3	Risposte ricevute tramite questionario online.....	13
4.4	Pareri scritti supplementari	14

Compendio

Nella seduta del 22 novembre 2023, il Consiglio federale ha adottato il messaggio concernente la nuova legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (legge sull'Id-e). Secondo quest'ultima, sarà la Confederazione a emettere i mezzi di identificazione elettronici (Id-e) e a gestire l'infrastruttura di fiducia necessaria. L'emissione degli Id-e dovrebbe cominciare all'inizio del 2026, in concomitanza con l'entrata in vigore della legge. Per rispettare tale termine occorre scegliere il prima possibile quale tecnologia utilizzare.

A questo scopo è stata avviata una consultazione pubblica, basata su un documento di discussione in cui sono state presentate e discusse due possibili varianti di attuazione, ognuna con i propri vantaggi e inconvenienti. Nella prima variante, la Svizzera seguirebbe ampiamente l'approccio previsto dall'Unione europea (UE), mentre, nella seconda, utilizzerebbe una tecnologia volta a proteggere ancor più la sfera privata degli utenti.

Nel quadro della consultazione sono pervenuti 97 pareri da autorità, partiti politici, organizzazioni e singoli cittadini. I risultati mostrano una ripartizione equilibrata delle preferenze tra i due scenari. Questa decisione richiede una complessa valutazione di diversi fattori, tra i quali la protezione dei dati, la sicurezza, l'interoperabilità e la fattibilità tecnica.

1 Situazione iniziale

Dopo l'esito negativo della votazione popolare del 7 marzo 2021 sulla legge federale sui servizi d'identificazione elettronica, il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia di delineare, in collaborazione con la Cancelleria federale e il Dipartimento federale delle finanze, una soluzione per un mezzo d'identificazione elettronico statale sicuro. Nel frattempo, il Consiglio nazionale e il Consiglio degli Stati hanno accolto sei identiche mozioni, depositate da tutti i gruppi parlamentari, che chiedevano la messa a punto di un sistema gestito dallo Stato atto a provare la propria identità in rete.

Desiderando coinvolgere da subito le cerchie interessate nell'elaborazione della nuova legge, nell'autunno 2021 l'Ufficio federale di giustizia ha avviato una consultazione pubblica informale. Fondandosi sui [pareri della procedura di consultazione](#), il 17 dicembre 2021 il Consiglio federale ha adottato una decisione di principio in cui ha posto le fondamenta del futuro Id-e. L'[avamprogetto di legge](#) è stato posto in consultazione dal 29 giugno 2022 al 20 ottobre 2022. Il 22 novembre 2023 il Consiglio federale ha adottato il [messaggio](#) e il disegno. Il 14 marzo 2024 il Consiglio nazionale ha accettato la legge sull'Id-e con 175 voti favorevoli, 12 contrari e 2 astensioni.

L'emissione degli Id-e dovrebbe cominciare all'inizio del 2026, in concomitanza con l'entrata in vigore della legge. Per rispettare tale termine occorre scegliere il prima possibile quale tecnologia utilizzare.

A questo scopo il team del progetto Id-e dell'UFG ha elaborato un documento di discussione, con la consulenza del Technical Advisory Circle, una cerchia di esperti istituita per beneficiare delle conoscenze e della rete della comunità svizzera dell'Id-e. Il documento di discussione contiene in particolare i seguenti punti:

- premessa: visione dell'UFG e riferimenti al contesto europeo;
- principi di sviluppo dell'Id-e e dell'infrastruttura di fiducia secondo il disegno;
- criteri di decisione;
- due possibili scenari: seguire la direzione tecnica dell'UE oppure rafforzare ulteriormente la protezione della sfera privata.

Il 1° dicembre 2023 è stato pubblicato su GitHub il [documento di discussione in inglese](#), mentre le traduzioni in [tedesco](#) e in [francese](#) sono state pubblicate successivamente. Lo stesso giorno è stato inviato via e-mail e newsletter Id-e l'invito alla consultazione, nel corso della quale sono state poste le domande seguenti:

- Qual è lo scenario preferito e perché?
- Entrambi gli scenari soddisfano le aspettative?
- In cosa consistono i rischi principali?
- Quali sono i limiti da non oltrepassare?

A queste domande si poteva rispondere compilando un questionario online, con la possibilità di aggiungere commenti e osservazioni. La presente valutazione considera i 97 pareri ricevuti fino al 22 gennaio 2024.

2 Risultati

Hanno partecipato alla consultazione 97 organizzazioni e persone. Tra queste, 85 hanno compilato solo il questionario online, 6 hanno compilato il questionario online ed espresso un parere supplementare e altre 6 hanno presentato soltanto un parere formulato liberamente.

Il 7 marzo 2024 sono stati pubblicati i risultati della consultazione su GitHub: un file Excel presenta le risposte del questionario online e un file PDF illustra i pareri scritti supplementari.

Un elenco dei partecipanti è reperibile in allegato.

2.1 Qual è lo scenario preferito e perché?

Da quanto emerge dall'analisi delle preferenze semplici, 46 partecipanti (47,4 %) sono a favore di un allineamento all'UE, mentre 46 (47,4 %) prediligono una protezione supplementare della sfera privata. Secondo 5 partecipanti (5,2 %) le informazioni disponibili non permettono ancora di prendere una decisione. (v. figura 1).

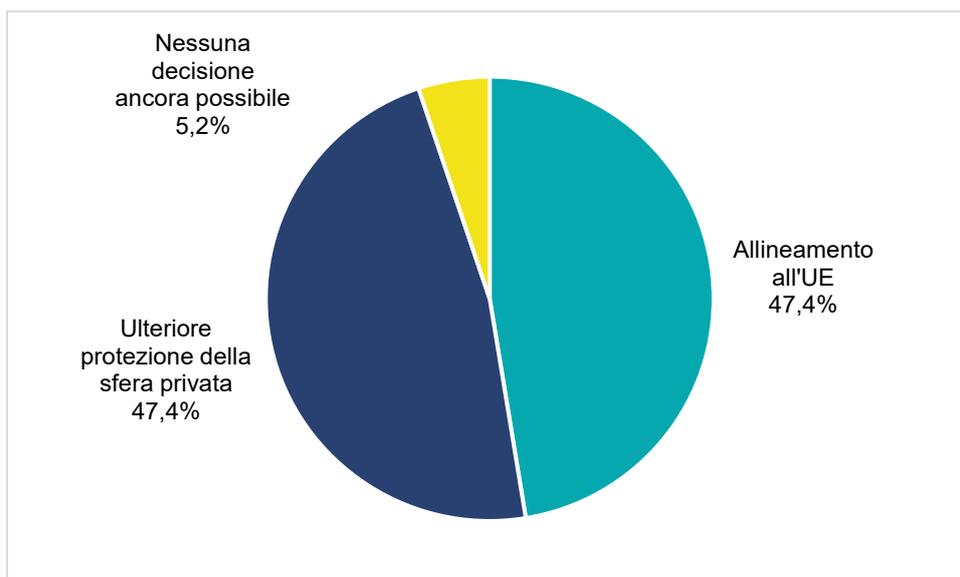


Figura 1: Preferenze semplici

Sostengono un allineamento all'UE: i Cantoni di Appenzello Interno, Basilea-Campagna, Basilea-Città, Obvaldo, San Gallo, Turgovia (Migrationsamt), Vallese, Vaud, Zugo, DIDAS, SICPA SA, Switch, Procivis AG, l'Unione delle città svizzere, Swisscom (Svizzera) SA, Ergon Informatik AG, Adnovum AG, Educa, le Ferrovie federali svizzere, l'Associazione svizzera degli ufficiali dello stato civile, l'Ufficio federale della sanità pubblica. Motivano la loro posizione in particolare con le seguenti considerazioni:

- interoperabilità agevolata con l'Unione europea;
- tecnologia e crittografia collaudate, resistenza post-quantistica;
- applicazione più semplice, economica e quindi veloce;
- grande comunità scientifica, rapido sviluppo dell'ecosistema.

Prediligono una protezione supplementare della sfera privata: i Cantoni di Argovia, Ginevra, Friburgo, Neuchâtel, Lucerna, San Gallo (Fachstelle für Datenschutz), Soletta, Svitto, Turgovia (Departement für Inneres und Volkswirtschaft, Kompetenzzentrum für Digitale Verwaltung), il PES, il PS, Abraxas Informatik AG, il PPS, CH++, Ubique, Swiss Fintech Innovations, l'EPFL, E-ID-Referendum, Società Digitale, la Posta svizzera e SwissSign AG, digitalswitzerland, IBM

Research, Swico, Information Security Society Switzerland, Vereign AG, Swiss Data Alliance, l'Unione svizzera delle arti e mestieri, Health Info Net AG, syndicom, l'Organizzazione degli Svizzeri all'estero, economiesuisse. Motivano la loro posizione in particolare con le seguenti considerazioni:

- protezione supplementare della sfera privata, soprattutto in materia di non collegabilità (unlinkability, traceability, non-correlation). Un esempio: una persona effettua una prima transazione e dimostra di essere maggiorenne, senza rivelare ulteriori informazioni come il nome o la data di nascita esatta. Il verificatore non riceve solo l'informazione «maggiore età», ma anche il materiale crittografico che rende il mezzo di autenticazione verificabile e unico. Quando si dimostra un'altra volta la propria età, la non collegabilità impedisce al verificatore di attribuire le due transazioni alla stessa persona; altrimenti sarebbe facile crearne il profilo;
- accettazione politica, minor rischio di un referendum con esito positivo;
- nessuna dipendenza dall'estero, specialmente dall'UE, i cui progetti non sono ancora chiari;
- la Svizzera può posizionarsi come pioniere in materia di protezione della sfera privata a livello internazionale.

I seguenti cinque Cantoni ritengono che le informazioni disponibili non permettono ancora di prendere una decisione: Appenzello Esterno, Berna, Glarona, Grigioni e Zurigo.

2.2 Entrambi gli scenari soddisfano le aspettative?

Dall'analisi delle preferenze esclusive risulta quanto segue: 25 partecipanti (26 %) sono favorevoli esclusivamente a seguire l'UE, mentre 28 (29 %) sono favorevoli esclusivamente a proteggere ulteriormente la sfera privata. Secondo 5 partecipanti (5 %) le informazioni disponibili non permettono ancora di prendere una decisione. 39 partecipanti (40 %) non hanno espresso alcuna preferenza esclusiva (v. figura 2).

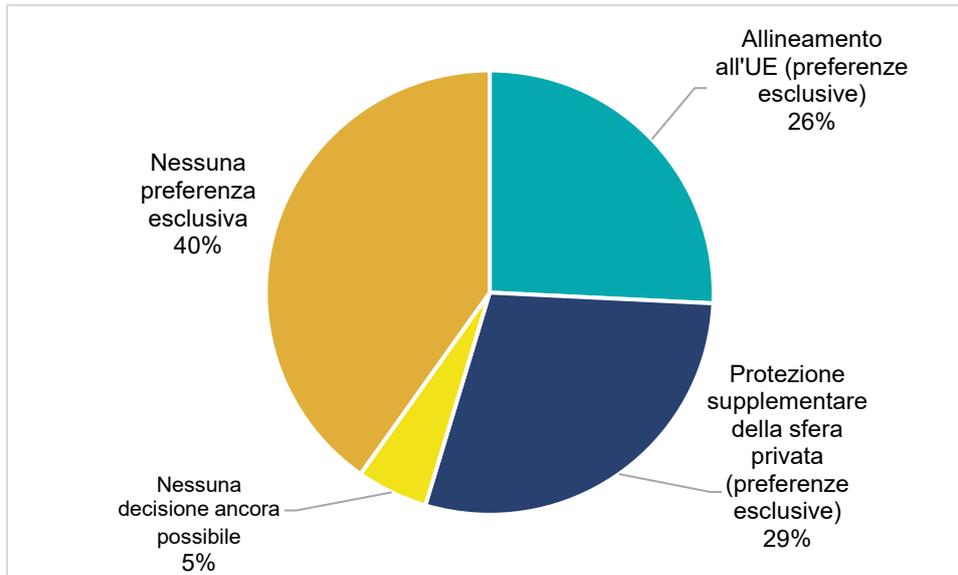


Figura 2: Preferenze esclusive

Sono favorevoli esclusivamente a seguire l'Unione europea: il Cantone di Obvaldo, l'Ufficio federale della sanità pubblica, la Federazione Svizzera degli Avvocati, DIDAS, l'Unione delle città svizzere, Interpension, Procivis AG, AdNovum AG, le Ferrovie federali svizzere.

Sono favorevoli esclusivamente a proteggere ulteriormente la sfera privata: i Cantoni di Argovia, Friburgo, Lucerna, Soletta, San Gallo (Fachstelle für Datenschutz), Turgovia (Departement für Inneres und Volkswirtschaft), il PS, il PES, Swiss Fintech Innovations, E-ID-Referendum, IBM Research, Information Security Society, l'Unione svizzera delle arti e mestieri, syndicom, Società Digitale, Verein AG, Health Info Net AG.

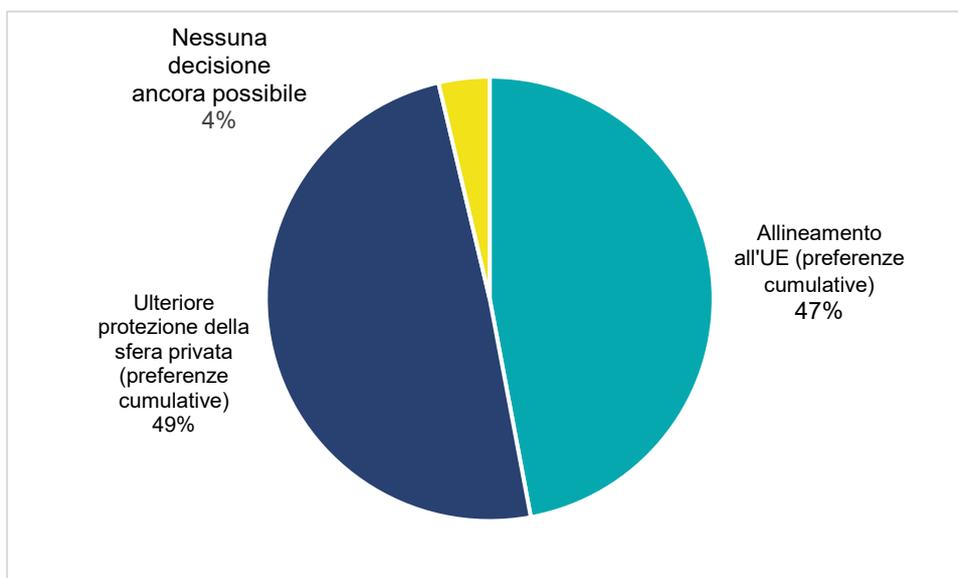


Figura 3: Preferenze cumulative

L'analisi delle preferenze cumulative mostra che 64 partecipanti (47 %) considerano l'allineamento all'Unione europea come prima o seconda scelta, mentre per 67 (49 %) lo è una maggiore protezione della sfera privata. Nell'approccio cumulativo, i 5 partecipanti secondo i quali le informazioni disponibili non permettono ancora di prendere una decisione hanno un peso relativo del 4 % (v. figura 3).

2.3 In cosa consistono i rischi principali?

I rischi menzionati nei pareri si possono raggruppare come segue.

- Rapidità della decisione: alcuni ritengono prematuro prendere una decisione sulla tecnologia da utilizzare e temono che una decisione presa in questo momento condurrebbe molto probabilmente in un vicolo cieco. Altri, invece, credono che ritardare la decisione metta a rischio l'Id-e e che sia decisivo iniziare la sua emissione il prima possibile: alcuni aggiustamenti successivi saranno in ogni caso inevitabili. In questo contesto si teme anche che seguire l'Unione europea possa portare a ritardi, nel caso in cui quest'ultima non avanzi come previsto.
- Rischi tecnici: secondo diversi partecipanti le tecnologie proposte non sono ancora mature, le standardizzazioni non sono ancora disponibili, la questione post-quantistica è irrisolta e il progetto risulta troppo complesso. Nel migliore dei casi si dovrebbero pertanto mettere in conto costi ingenti e ritardi. A tutto ciò si associa anche il rischio che le comunità impegnate a sviluppare queste tecnologie siano troppo piccole. Tra i rischi tecnici si ipotizza anche una dipendenza dal percorso. Nel documento di discussione si considera la possibilità di fare ricorso al multi-stack, ovvero la capacità di operare su più binari tecnologici. Tuttavia, in riferimento alla dipendenza dal percorso si sostiene che, scegliendo inizialmente di conformarsi all'Unione europea sarebbe difficile o addirittura impossibile rafforzare ulteriormente la protezione della sfera privata in un secondo momento.
- Rischi legati all'hardware: con particolare riguardo ai dispositivi in cui si salvano i dati, gli smartphone degli utenti, diverse parti segnalano il pericolo di dipendenza da hardware e software proprietari, talvolta non trasparenti. Inoltre, i criptoprocessori degli smartphone non supportano tutti i tipi di firma eventualmente auspicabili.
- Fallimento politico: alla luce degli antecedenti legati all'Id-e, molti temono un nuovo fallimento alle urne e sostengono pertanto la variante che protegge ulteriormente la sfera

privata. Altri, invece, ritengono che quest'ultima variante contenga soluzioni il cui valore sarebbe tutt'al più accademico e temono quindi il rischio d'inseguire una chimera.

- Isolamento della Svizzera: secondo alcuni, vi è il rischio che la variante volta a proteggere ulteriormente la sfera privata rischi di attirare coloro che criticano di principio le proposte dell'UE e prediligono una soluzione indipendente.
- Altri rischi: nei pareri sono menzionati anche l'eccesso d'identificazione, la fuga di dati, la difficoltà d'uso e la mancanza di possibilità di applicazione.

2.4 Quali sono i limiti da non oltrepassare?

Le risposte a questa domanda riflettono i risultati dell'analisi delle preferenze esclusive. Nel capitolo 2.2 si vede che il 26 % dei partecipanti è esclusivamente favorevole a conformarsi all'UE, mentre il 29 % preferisce una protezione supplementare della sfera privata. Allo stesso tempo, è da notare che il 40 % dei partecipanti non esprime alcuna preferenza esclusiva e il 5 % considera il momento della decisione prematuro.

Analogamente, il limite da non oltrepassare sarebbe per alcuni partecipanti un allontanamento dall'UE mentre per altri un compromesso sulla protezione dei dati e la sicurezza. In questo contesto, molti menzionano la non collegabilità dei mezzi di autenticazione, o meglio, della presentazione ripetuta dello stesso mezzo di autenticazione.

In generale, va tuttavia constatato che molte formulazioni fanno riferimento ai rischi (v. 2.3) e non menzionano dei veri e propri limiti da non oltrepassare. Vengono piuttosto formulate raccomandazioni come:

- qualsiasi compromesso va comunicato in modo trasparente e motivato;
- laddove possibile, vanno favorite soluzioni che possano essere adattate con la massima flessibilità possibile agli sviluppi futuri;
- la fattibilità politica va sempre tenuta in conto;
- vanno privilegiate le soluzioni che favoriscono un alto livello di diffusione anche nel settore privato.

2.5 Altre osservazioni

In un campo libero alla fine del formulario i partecipanti hanno potuto esprimere ulteriori riflessioni, in molte delle quali riemergono i temi dei capitoli 2.3 e 2.4. Sono inoltre particolarmente degni di nota i seguenti commenti.

- Si propone di emettere l'Id-e sotto forma di mezzo di autenticazione sia qualificato che significativo, eventualmente con attributi diversi.
- Si richiede un collegamento stretto o almeno una semplificazione significativa dell'accesso a una firma elettronica qualificata.
- Sebbene l'holder binding, ovvero il collegamento tra l'utente, il dispositivo, il portafoglio elettronico e il mezzo di autenticazione sia indiscutibilmente di grande importanza, è da evitare che questo porti a un manufacturer binding.
- Lo sviluppo dell'ecosistema, che annovera numerosi emittenti e verificatori, riveste grande importanza e la Confederazione dovrebbe assumersi le proprie responsabilità in questo ambito.
- La ricerca criptografica in Svizzera, che ricopre già una posizione eccellente, va ulteriormente potenziata in vista della sua crescente importanza.
- Non da ultimo, diversi partecipanti offrono ulteriore sostegno o collaborazione nello sviluppo della prevista infrastruttura di fiducia.

3 Osservazioni finali

I risultati mostrano una distribuzione equilibrata delle preferenze tra i due scenari. Questa decisione richiede una valutazione complessa di diversi fattori, tra i quali la protezione dei dati, la sicurezza, l'interoperabilità e la fattibilità tecnica.

Dimostrano inoltre la grande competenza dei partecipanti alla presente consultazione: un fattore da non sottovalutare in vista del dibattito pubblico sull'Id-e e sulla relativa infrastruttura di fiducia, nonché sullo sviluppo di un ecosistema di mezzi di autenticazione elettronici.

4 Allegati

4.1 Membri del Technical Advisory Circle (TAC)

Il TAC si è riunito tre volte online. I verbali si possono consultare su GitHub ai seguenti link:

- [21 settembre 2023](https://github.com/e-id-admin/general/blob/main/meetings/20230921_TAC_Meetingminutes.pdf)
(https://github.com/e-id-admin/general/blob/main/meetings/20230921_TAC_Meetingminutes.pdf)
- [16 ottobre 2023](https://github.com/e-id-admin/general/blob/main/meetings/20231016_TAC_Meetingminutes.pdf)
(https://github.com/e-id-admin/general/blob/main/meetings/20231016_TAC_Meetingminutes.pdf)
- [9 novembre 2023](https://github.com/e-id-admin/general/blob/main/meetings/20231109_TAC_Meetingminutes.pdf)
(https://github.com/e-id-admin/general/blob/main/meetings/20231109_TAC_Meetingminutes.pdf)

4.2 Elenco dei partecipanti alla consultazione

Cantoni

- Cantone di Argovia
- Cantone di Appenzello Esterno
- Cantone di Appenzello Interno
- Cantone di Basilea-Campagna
- Cantone di Basilea-Città
- Cantone di Berna
- Cantone di Friburgo
- Cantone di Ginevra
- Cantone di Glarona
- Cantone dei Grigioni
- Cantone di Lucerna
- Cantone di Neuchâtel
- Cantone di Obvaldo
- Cantone di Svitto
- Cantone di Soletta
- Cantone di San Gallo
- Cantone di San Gallo, Fachstelle für Datenschutz
- Cantone di Turgovia, Departement für Inneres und Volkswirtschaft
- Cantone di Turgovia, Kompetenzzentrum Digitale Verwaltung
- Cantone di Turgovia, Migrationsamt
- Cantone di Vaud
- Cantone del Vallese
- Cantone di Zugo
- Cantone di Zurigo

Autorità

- Ufficio federale della sanità pubblica, Divisione Trasformazione digitale

- Ufficio federale della sanità pubblica, Sezione Sanità Digitale

Partiti politici

- VERDI svizzeri (PES)
- Partito Pirata Svizzero (PPS)
- Partito socialista svizzero (PS)

Comunità scientifica

- Beer Carolin, Schaller Patrick e Čapkun Srdjan (tutti del PFZ)
- PFL
- Fehrensens, Benjamin (BFH)
- HES-SO
- Laube, Annett (BFH)

Altre cerchie

- Abraxas Informatik AG, Christian Werder
- Abraxas Informatik AG, Silvano Fari
- Adnovum AG
- Associazione svizzera degli ufficiali dello stato civile
- Organizzazione degli Svizzeri all'estero
- Commissione extraparlamentare Forum PMI
- besec.digital AG
- CH++
- DIDAS
- Società Digitale
- digitalswitzerland
- economiesuisse
- Educa
- E-ID-Referendum
- Ergon Informatik AG
- FutureITcom GmbH
- gigmade AG
- Health Info Net AG
- Hoewler Consulting
- IBM Research
- Information Security Society Switzerland
- Inova Solutions AG
- Netcetera AG, Veridos AG, Blokverse
- Procivis AG
- Rigiblue
- Samsung Electronics Switzerland GmbH
- Schweidt & Bachmann Schweiz
- Ferrovie federali svizzere FFS
- Federazione Svizzera degli Avvocati

- Unione svizzera delle arti e mestieri
- Unione delle città svizzere
- SICPA SA
- SORBA EDV AG
- Swico
- Swiss Data Alliance
- Swiss Fintech Innovations
- La Posta svizzera SA, SwissSign AG
- Swisscom (Svizzera) SA
- Switch
- syndicom
- Ubique AG
- Vereign AG
- Associazione eGov-Svizzera
- Associazione dei servizi della navigazione

Singoli cittadini

- Aeschlimann, Andres
- Anonimo 1
- Anonimo 2
- Anonimo 3
- Anonimo 4
- Anonimo 5
- Blume, Matthias
- Christen, Tobias
- Dunant, Raphaël
- Fiore, Nico
- Furrer, Bruno
- Gfeller, S.
- Grossenbacher, Samuel
- Keil, Hartmut
- Keller, Philippe
- Oeri, Hans-Peter
- Šarinay, Juraj
- Schnyder, Stéphane
- Suvorov, Vasily

4.3 Risposte ricevute tramite questionario online

Le risposte pervenute tramite questionario online sono pubblicate in un file Excel separato su Github:

https://github.com/e-id-admin/open-source-community/blob/main/discussion-paper-tech-proposal/20240307_discussion_paper_tech_proposal_responses.xlsx

4.4 Pareri scritti supplementari

I pareri scritti supplementari sono pubblicati in un file PDF separato su Github:

https://github.com/e-id-admin/open-source-community/blob/main/discussion-paper-tech-proposal/20240307_discussion_paper_tech_proposal_additional_statements.pdf