CONFERENZA DELLE REGIONI
E DELLE PROVINCE AUTONOME

26/62/SR16/C14

POSIZIONE SULLO SCHEMA DI DECRETO DEL SOTTOSEGRETARIO DI STATO ALLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI CON DELEGA ALL'INNOVAZIONE TECNOLOGICA E LA TRANSIZIONE DIGITALE, DI CONCERTO CON IL MINISTRO DELL'ECONOMIA E DELLE FINANZE E IL MINISTRO PER LA PUBBLICA AMMINISTRAZIONE, DI APPROVAZIONE DELLE LINEE GUIDA DEL SISTEMA IT-WALLET E REGOLE PER LA SPERIMENTAZIONE

Parere, ai sensi dell'articolo 64-quater, comma 3, del decreto legislativo 7 marzo 2005, n. 82

Punto 16) O.d.g. Conferenza Stato-Regioni

La Conferenza delle Regioni e delle Province autonome esprime parere favorevole sullo schema di decreto in oggetto, con le raccomandazioni di seguito riportate.

Raccomandazioni

1) All'**articolo 1, comma 1, lettera b)**, la formulazione vigente della definizione di Attestato Elettronico di Attributi presenta profili di ambiguità interpretativa, in quanto non consente di distinguere in modo chiaro e sistematico tra Attestato Elettronico di Attributi Pubblici e Attestato Elettronico di Interesse Pubblico. In particolare, la definizione attuale utilizza criteri eterogenei e non esplicitamente coordinati da un lato, la provenienza dell'attributo (derivazione da Fonte Autentica pubblica), dall'altro, la funzione giuridica dell'attestazione (valore fiduciario e tutela della fede pubblica). Tali criteri, non essendo distinti in modo chiaro, possono determinare sovrapposizioni applicative e incertezze nella qualificazione delle attestazioni, con possibili riflessi sull'individuazione dei requisiti tecnici e di sicurezza, sulla corretta attribuzione delle responsabilità e sull'interpretazione degli effetti giuridici delle attestazioni.

2) La proposta di riformulazione interviene pertanto al fine di distinguere in modo esplicito il criterio oggettivo della provenienza del dato (Fonte Autentica pubblica), il criterio funzionale della rilevanza giuridica dell'attestazione (valore probatorio e tutela della fede pubblica) e chiarire che le due qualificazioni possono, ove ne

ricorrano i presupposti, coesistere nel medesimo attestato, evitando interpretazioni restrittive o incoerenti;

3) All'**articolo 1**, la definizione di Soggetti aggregatori, secondo la definizione vigente, si riferisce alle sole Soluzioni Tecniche di verifica, non coprendo le funzioni di raccordo organizzativo e tecnico che le infrastrutture regionali di autenticazione svolgono per abilitare i Verificatori aggregati alla fruizione del Sistema. Le Specifiche Tecniche del Sistema IT-Wallet (sezione "10.3. Soluzione di Relying Party", disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/) disciplinano esplicitamente tali funzioni con la figura dell'"Intermediario di Relying Party", coincidente con il broker regionale, ma non rispecchiata nella norma primaria. La definizione aggiornata è il presupposto per disciplinare il percorso di registrazione nel Registro IT-Wallet per questi soggetti, attualmente assente dalle Specifiche Tecniche del Sistema IT-Wallet (sezione "8.1.2. Tipi di Entità e percorsi di Onboarding", Tabella 8.1, disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/).

4) All'**articolo 3, comma 3,** si raccomanda di esplicitare che gli aggiornamenti delle Linee Guida e delle Specifiche Tecniche che riguardano i requisiti dei Soggetti Aggregatori, le modalità di accesso tramite PDND, le procedure di registrazione delle Fonti Autentiche regionali o il coordinamento dei flussi di delega producono effetti diretti sulle infrastrutture digitali regionali, venga sempre previsto il coinvolgimento della Conferenza Unificata.

5) L'**articolo 4, comma 1, lettera h)**, include i Soggetti Aggregatori come figura accessoria ai Verificatori di Attestati Elettronici, senza riconoscerne l'autonomia organizzativa e tecnica. Tale impostazione non tiene conto del fatto che i Soggetti Aggregatori, in particolare le infrastrutture regionali di autenticazione, gestiscono in modo centralizzato centinaia di Verificatori di Attestati Elettronici e migliaia di servizi, con un ruolo funzionale distinto rispetto al singolo Verificatore. Senza una registrazione autonoma nel Registro IT-Wallet, il Soggetto Aggregatore non ha una propria identità giuridica e tecnica nel Sistema: è costretto a operare con il materiale crittografico di ciascun Verificatore che rappresenta, rendendo necessario replicare la registrazione per ciascun Verificatore, con un onere operativo piuttosto gravoso per le infrastrutture regionali.

6) All'**articolo 5,** il **comma 3** attribuisce ad AgID il potere di registrare i soggetti nel Registro IT-Wallet ma non prevede alcun obbligo di pubblicità degli esiti, né un termine per l'aggiornamento del Registro. In un sistema multi-attore in cui centinaia di Soggetti Aggregatori gestiscono migliaia di Verificatori di Attestati Elettronici, la trasparenza del Registro è condizione necessaria per la fiducia degli Utenti e per la verificabilità delle catene di responsabilità. In particolare, l'Utente che interagisce con un servizio tramite Wallet deve poter verificare se il Soggetto Aggregatore che

gestisce l'accesso è regolarmente registrato e per quali Attestati è autorizzato a operare. L'emendamento recepisce i principi di trasparenza dell'azione amministrativa (art. 1 della legge n. 241/1990) applicandoli al contesto del Registro IT-Wallet.

7) Rispetto all'**articolo 6, comma 1, lettera a),** si raccomanda di prescrivere un contenuto minimo per le Specifiche Tecniche. In particolare, le Specifiche Tecniche descrivono la figura dell'Intermediario di Relying Party nella sezione dedicata alla Soluzione di Relying

Party, ma non prevedono né un percorso di registrazione autonomo per questi soggetti né un loro ruolo nella federazione di trust, come risulta dalla tabella dei percorsi di onboarding e dalla tabella dei ruoli di federazione. Senza questa disciplina, la figura introdotta con gli emendamenti numero 1 e 2 resta priva di attuazione tecnica.

8) Il **comma 3** dell'**articolo 6** definisce il contenuto del Regolamento AgID in materia di registrazione dei soggetti al Sistema, ma non include tre discipline necessarie per l'operatività del Sistema a regime. 1) il rapporto tra il Soggetto Aggregatore e i Verificatori che rappresenta configura un rapporto titolare-responsabile del trattamento ai sensi dell'articolo 28 del Regolamento (UE) 2016/679, che impone la formalizzazione per iscritto con contenuto minimo. Le Linee Guida (§2.2.7) lasciano tali accordi alla contrattazione libera, producendo un vuoto di accountability che AgID non può colmare in sede di vigilanza. 2) le Specifiche Tecniche descrivono i requisiti di ciascun componente del Sistema ma non definiscono uno schema di relazione tecnica da allegare all'istanza di registrazione. Senza un contenuto minimo normativo differenziato per categoria di soggetto, AgID potrebbe applicare agli enti pubblici regionali gli stessi oneri documentali previsti per un fornitore privato di attestati, pur trattandosi di soggetti con caratteristiche organizzative e di responsabilità diverse. 3) la norma li qualifica espressamente come "compatibili con la disciplina europea dei Soggetti Privati", ma non esclude che AgID li applichi anche ai Soggetti Pubblici. Le garanzie assicurative sono uno strumento del diritto privato difficilmente applicabile agli enti pubblici, la cui affidabilità è garantita dalla natura giuridica pubblica e dai controlli istituzionali cui sono già soggetti per legge. L'emendamento chiarisce che per i Soggetti Pubblici questi requisiti vanno declinati in modo coerente con la loro natura, con esclusione esplicita delle garanzie assicurative.

9) Al **Par. 4.5 delle Linee Guida** La disposizione vigente pone in capo ai Titolari di Fonti Autentiche l'obbligo di *"garantire la qualità dei dati anagrafici o Attributi erogati"*, senza tuttavia specificare il contenuto giuridico e operativo di tale requisito. Il concetto di "qualità del dato", così formulato, presenta profili di genericità e indeterminatezza, in quanto non individua parametri oggettivi e verificabili, non chiarisce quali obblighi concreti gravino sul Titolare di Fonte Autentica e può

determinare applicazioni non uniformi tra le diverse amministrazioni. In particolare, l'assenza di una definizione esplicita può generare incertezza nella valutazione della conformità delle basi dati nella delimitazione delle responsabilità, nella gestione dei processi di aggiornamento e rettifica delle informazioni. La riformulazione proposta consente pertanto di rafforzare la certezza giuridica, l'uniformità applicativa tra amministrazioni, la coerenza con i principi in materia di protezione dei dati personali (in particolare, accuratezza e integrità dei dati ai sensi del GDPR) e soprattutto l'affidabilità complessiva del sistema IT-Wallet.

10) Le **Linee Guida (§3.1)** descrivono tre stati dell'Istanza IT-Wallet, installato, operativo, attivo senza spiegare le precondizioni per ciascuno. Le Specifiche Tecniche del Sistema IT-Wallet (sezione "10.1.4.1. Ciclo di vita dell'Istanza del Wallet", disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/) definiscono invece quattro stati con precondizioni esplicite: Installato (App scaricata ma non ancora attivata); Operativo (App attivata, dispositivo verificato, Wallet Attestation ricevuto, ma senza Documento di Identità Digitale); Valido (Documento di Identità Digitale ottenuto, istanza pienamente operativa); Disinstallato. Il termine "attivo" delle Linee Guida corrisponde allo stato "Valido" delle Specifiche Tecniche. Un'istanza nello stato Operativo ha capacità limitate: può avviare la procedura di ottenimento del PID e richiedere Attestati Elettronici che non richiedono il PID, ma non può presentare il PID ai Verificatori. Un'istanza nello stato Valido è pienamente operativa. Questa differenza è rilevante per i Soggetti Aggregatori, che devono verificare lo stato dell'istanza prima di avviare le interazioni con gli Utenti. Il disallineamento terminologico tra i due documenti genera confusione operativa. Si raccomanda di allineare la terminologia delle Linee Guida a quella delle Specifiche Tecniche o di esplicitare la corrispondenza tra i due sistemi.

11) Le **Linee Guida (sezione 2.2.7)** prescrivono che i Verificatori di Attestati Elettronici "devono autenticare" i dati ricevuti ma "dovrebbero verificarne lo stato di validità", introducendo una distinzione di forza normativa tra i due obblighi che non trova giustificazione nell'architettura del Sistema. Nel modello corretto del Sistema IT-Wallet la garanzia che un Attestato presentato sia valido non è un onere del Verificatore: è una responsabilità del Wallet dell'Utente e del Fornitore di Attestati Elettronici, che gestiscono il ciclo di vita degli Attestati e devono impedire la presentazione di Attestati scaduti, revocati o sospesi. Il Verificatore riceve un Attestato che il Sistema ha già garantito essere valido: aggiungergli l'onere di verificarne autonomamente lo stato introduce una ridondanza che rallenta il flusso e scarica sul Verificatore una responsabilità che non gli appartiene. Si raccomanda che le Linee Guida chiariscano che la validità dell'Attestato al momento della presentazione è garantita dal Sistema, dal Wallet e dal Fornitore di Attestati Elettronici, e che il Verificatore non è tenuto a effettuare controlli autonomi sullo stato di validità, potendo fare affidamento su quanto attestato dal Sistema stesso.

12) Le Specifiche Tecniche del Sistema IT-Wallet (sezione “16.1.3. Politica di Conservazione dei Log della Relying Party”, disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/) prevedono che i Verificatori di Attestati Elettronici possano conservare i log relativi ai dati ricevuti dal Wallet per un massimo di ventiquattro mesi, e che non dovrebbero registrare le mappe di divulgazione degli Attestati ove non necessario. Il decreto non contiene disposizioni equivalenti: né i tipi di eventi da registrare obbligatoriamente, né i periodi minimi di conservazione, né le misure di sicurezza applicabili, né le modalità con cui AgID può accedere ai log in sede di vigilanza. Affidare questa disciplina alle sole Specifiche Tecniche significa che AgID non dispone di una base certa su cui fondare le verifiche previste dall'articolo 7, e che i soggetti registrati non hanno obblighi chiari e uniformi in materia. Si segnala inoltre un problema specifico che né il decreto né le Specifiche Tecniche affrontano: la registrazione del codice fiscale o codice identificativo ANPR nei log di sessione equivale alla registrazione di un Attributo dell'Utente, anche senza annotare le mappe di divulgazione degli Attestati presentati. Si raccomanda che il Regolamento IT-Wallet definisca:

    - i tipi di eventi che i Verificatori sono obbligati a registrare;
    - i periodi minimi di conservazione, differenziati per categoria di dato trattato;
    - le misure minime di sicurezza;
    - le modalità di accesso ai log da parte di AgID in sede di vigilanza.

13) Le Specifiche Tecniche del Sistema IT-Wallet (sezione “8.2.1. Requisiti di Registrazione AS”, disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/) prescrivono che i Titolari di Fonte Autentica dichiarino i propri Attributi nel Registro delle Fonti Autentiche usando tipi di dato già presenti nel Registro dei Claims. Il Registro dei Claims (sezione “7.3. Registro dei Claims” delle Specifiche Tecniche del Sistema IT-Wallet, disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/) contiene le definizioni standardizzate degli attributi già previsti dagli standard nazionali ed europei. Per eventuali Attributi di esclusiva pertinenza regionale, i corrispondenti tipi di dato non sono ancora nel Registro dei Claims. Le Specifiche Tecniche non definiscono né la procedura per proporre nuovi tipi di dato né l'organo competente a valutarle: si riferiscono genericamente a un “Organismo di Supervisione” senza identificarlo. Si raccomanda che le Specifiche Tecniche definiscano:

    - la procedura di proposta di nuovi tipi di dato;
    - l’organo competente a valutarle, con i criteri e i termini di risposta;
    - un percorso semplificato per i Soggetti Pubblici con Attributi regionali già strutturati in archivi istituzionali.

14) Le Specifiche Tecniche del Sistema IT-Wallet (sezione “10.3. Soluzione di Relying Party”, disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/) descrivono la figura dell'Intermediario di Relying Party come un soggetto che può agire per conto di un Verificatore di Attestati Elettronici, mettendogli a disposizione i servizi tecnici necessari per collegarsi all'Istanza IT-Wallet degli Utenti. È esattamente il ruolo che le infrastrutture regionali di autenticazione svolgono per centinaia di enti. Tuttavia, la tabella dei percorsi di registrazione (Specifiche Tecniche del Sistema IT-Wallet, sezione “8.1.2. Tipi di Entità e percorsi di Onboarding”, Tabella 8.1) non include l'Intermediario di Relying Party tra i soggetti che possono registrarsi nel Sistema: vi figurano le Fonti Autentiche, i Fornitori di Attestati Elettronici, i Verificatori di Attestati Elettronici e i Fornitori di Wallet, ma non gli Intermediari. Anche la tabella dei ruoli nella federazione di trust (sezione “6.1. Ruoli di Federazione” delle Specifiche Tecniche del Sistema IT-Wallet (disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/)) non include questa figura. La conseguenza pratica è che un'infrastruttura regionale che operi come Intermediario per centinaia di Verificatori dovrebbe gestire un certificato crittografico distinto per ciascun Verificatore che rappresenta, senza potersi registrare come soggetto autonomo, con un onere operativo poco sostenibile su scala regionale e che rende di fatto inattuabile il modello centralizzato di gestione dell'autenticazione che caratterizza le infrastrutture pubbliche regionali. Si raccomanda che le Specifiche Tecniche definiscano: un percorso di registrazione autonomo per gli Intermediari di Relying Party; il loro ruolo nella federazione; le modalità di gestione del materiale crittografico per i Verificatori aggregati.

15) Le Specifiche Tecniche del Sistema IT-Wallet (sezioni “11.2. Modello di Dati del PID” e “11.1.2. Formato Attestato Elettronico SD-JWT-VC”, disponibili all'indirizzo https://italia.github.io/eid-wallet-it-docs/versione-corrente/it/) prevedono nel Documento di Identità Digitale (PID) tre identificatori distinti per lo stesso Utente:

    a. il claim sub, valore opaco che cambia per ogni credenziale emessa e garantisce che presentazioni diverse dello stesso PID non siano collegabili tra loro;

    b. il codice fiscale (tax_id_code), dato stabile divulgabile selettivamente;

    c. il codice identificativo ANPR (personal_administrative_number), dato stabile anch'esso divulgabile selettivamente.

La coesistenza di tre identificatori con caratteristiche così diverse non è spiegata nelle Linee Guida né nei DPCM. Ne derivano tre problemi pratici.

1) i Verificatori che richiedono sistematicamente il codice fiscale o il codice ANPR possono collegare tra loro sessioni diverse dello stesso Utente,

vanificando la protezione della privacy garantita dal claim sub; ma nessuna norma definisce quando un Verificatore può richiedere questi dati stabili.

2) Verificatori e Soggetti Aggregatori non sanno quale identificatore registrare nei log di sessione: usare il codice fiscale equivale a registrare un dato personale stabile dell'Utente, mentre usare il sub opaco è più coerente con il principio di minimizzazione.

3) Se l'emendamento Articolo 6 comma 1 lettera f viene accolto e il codice ANPR è aggiunto al PID come dato obbligatorio, il PID conterrà due identificatori stabili, rendendo ancora più necessaria una disciplina chiara delle condizioni di divulgazione di ciascuno.

Si raccomanda che le Specifiche Tecniche definiscano: a) le condizioni in cui i Verificatori possono richiedere il codice fiscale e/o il codice ANPR; b) quale identificatore usare nei log di sessione; c) la spiegazione esplicita della differenza funzionale tra i tre identificatori.

16) Le **Linee Guida (sezione 2.2.7)** impongono ai Verificatori di Attestati Elettronici di consentire all'Utente di richiedere la cancellazione dei Dati di Identificazione Personale e degli Attributi presentati. Il Sistema IT-Wallet è però progettato affinché i Verificatori non conservino i dati dell'Utente oltre la singola sessione di autenticazione. Per chi non conserva dati, l'obbligo non ha oggetto. Per chi invece li conserva per legittimo interesse o specifici obblighi normativi, il diritto alla cancellazione è già garantito dall'articolo 17 del Regolamento (UE) 2016/679 indipendentemente da questa previsione delle Linee Guida. Si raccomanda che le Linee Guida chiariscano: se l'obbligo presuppone la conservazione dei dati oltre la sessione; eventualmente come debba essere adempiuto da un Verificatore che non conserva dati; il coordinamento con l'articolo 17 del Regolamento (UE) 2016/679 per evitare sovrapposizioni.

17) L'**articolo 8, comma 2,** prevede che al termine della Sperimentazione i soggetti aderenti sottopongano alla valutazione di AgID i risultati tecnici conseguiti, senza definire né i criteri di valutazione né le conseguenze per i soggetti partecipanti. Non è disciplinato quando si considera conclusa la Sperimentazione, con quali parametri AgID valuta i risultati, se una valutazione positiva costituisce titolo preferenziale per la registrazione nel regime definitivo né cosa comporti una valutazione negativa. Il comma 3 precisa, inoltre, che l'ammissione alla Sperimentazione non genera alcun affidamento sul futuro riconoscimento del valore giuridico delle scelte tecnologiche compiute, lasciando i soggetti che hanno investito nell'adeguamento delle proprie infrastrutture senza certezza alcuna sull'esito del percorso intrapreso. Questa clausola lascia i soggetti pubblici regionali, che hanno investito nella costruzione di infrastrutture di autenticazione compatibili con il Sistema IT-Wallet, esposti al rischio di dover rivedere le proprie scelte tecnologiche senza preavviso e senza criteri predefiniti. Si raccomanda che il Regolamento IT-Wallet definisca i criteri di

valutazione degli esiti della Sperimentazione; le modalità con cui AgID comunica i risultati, le conseguenze ai fini della registrazione nel regime definitivo e un termine certo per la conclusione della valutazione.

18) Al **Par. 2.2.4** si dice che "*Il Titolare di Fonte Autentica PUÒ richiedere al Fornitore di Attestati Elettronici di Attributi una prova di Autenticazione dell'Utente per il rilascio degli Attributi a questo riferiti. In questo caso per l'emissione degli Attestati Elettronici di Attributi, il Fornitore di Attestati Elettronici di Attributi, DEVE Autenticare, mediante i suoi Dati di Identificazione Personale, l'Utente sulla base del Livello di Garanzia richiesto dal Titolare di Fonte Autentica*"**.** Con riferimento alla disposizione secondo cui: *"Il Titolare di Fonte Autentica può richiedere […] una prova di autenticazione dell'utente […] sulla base del livello di garanzia richiesto"*, si rileva che la formulazione attuale presenta profili di indeterminatezza sotto il profilo giuridico e applicativo, in particolare per quanto concerne i criteri di determinazione del livello di garanzia richiesto, il grado di discrezionalità attribuito al Titolare di Fonte Autentica, la relazione tra livello di garanzia e tipologia di servizio o attestazione.

Si rappresenta la necessità di chiarire:

- se il livello di garanzia debba essere: uniformemente definito a livello nazionale, oppure rimesso alla valutazione del Titolare di Fonte Autentica;
- se nell'ambito dell'accesso ai servizi digitali e del rilascio di attestazioni debba essere richiesto sempre il livello massimo disponibile, oppure sia consentita una modulazione del livello in funzione del rischio;
- se siano previsti criteri oggettivi e standardizzati, quali ad esempio: natura e rilevanza giuridica dell'attestazione; impatto sui diritti dell'interessato; rischio di utilizzo improprio o fraudolento; coerenza con i livelli di garanzia previsti dal regolamento (UE) n. 910/2014 (*eIDAS*).

19) Al **Par. 4.5**, Con riferimento agli obblighi posti in capo ai Titolari di Fonte Autentica in materia di esposizione dei servizi tramite PDND, abilitazione dei Fornitori di Attestati Elettronici, aggiornamento e notifica dei dati e degli attributi, si rileva che il quadro attuale disciplina in modo puntuale gli aspetti tecnici e di interoperabilità, ma non contempla esplicitamente un modello strutturato di gestione delle richieste e dell'assistenza nell'ambito dell'ecosistema IT-Wallet. Tale lacuna assume particolare rilevanza in considerazione della pluralità degli attori coinvolti, tra cui: Utenti (cittadini); Titolari di Fonti Autentiche; Fornitori di Attestati Elettronici; Verificatori; Gestori dei registri e delle infrastrutture centrali. Si evidenzia la necessità di prevedere un modello organizzativo e operativo di assistenza, volto a garantire la

gestione coordinata delle richieste provenienti dai diversi attori, la corretta attribuzione delle responsabilità nella risoluzione delle problematiche, la tracciabilità delle segnalazioni e degli interventi e la continuità operativa dei servizi. In assenza di un modello strutturato, si rilevano possibili criticità in termini di frammentazione dei punti di contatto, difficoltà di individuazione del soggetto competente, inefficienze nella gestione delle richieste, impatti negativi sull'esperienza utente e sull'affidabilità del sistema.

Roma, 29 aprile 2026