Ministero degli Affari Esteri
e della Cooperazione Internazionale

PORTALE VOTO ELETTRONICO

RELAZIONE FINALE

Indice dei contenuti

INDICE DELLE FIGURE E TABELLE **3**
Figure 3
Tabelle 3

PREMESSA **4**

1 INTRODUZIONE AL DOCUMENTO **5**
1.1 Termini, definizioni e acronimi 5

2 INTRODUZIONE AL PORTALE VOTO ELETTRONICO **6**

3 CRITICITÀ AFFRONTATE E PROPOSTE DI SOLUZIONE **7**
3.1 Infrastruttura 7
3.2 Criticità dell'Infrastruttura 8
3.3 Criticità blockchain 8
3.4 Criticità sessioni di collaudo 10
3.5 Criticità emerse a seguito dei Penetration Test 10
3.6 Criticità sulla pubblicazione del codice sorgente su GitHub 11
3.7 Criticità sulla segretezza del voto 12
3.8 Criticità sull'integrità e sulla verificabilità del voto 12
3.9 Criticità sulle operazioni di spoglio 12
3.10 Criticità sulla disponibilità del servizio 13
3.11 Criticità sull'helpdesk 13
3.12 Criticità sui fornitori 13

4 CONCLUSIONI **14**
4.1 Successo dell'opzione su Fast It 14
4.2 Successo della modalità di voto: 14
4.3 Conclusioni dell'analisi tecnica 15

INDICE DELLE FIGURE E TABELLE

FIGURE

Figura 1 - Architettura portale IoVoto 7
Figura 2 - Architettura cloud 7
Figura 3 - Distribuzione della gravità delle vulnerabilità 11
Figura 4 - Optanti per fasce di età 14

TABELLE

Tabella 1 - Termini e Acronimi 5
Tabella 2 - Optanti delle sedi sperimentanti 9
Tabella 3 - Vulnerabilità 11

PREMESSA

La legge 30 dicembre 2020, n. 178, recante il bilancio di previsione dello Stato per l'anno finanziario 2021 e il bilancio pluriennale per il triennio 2021-2023, ha autorizzato la spesa di 9 milioni di euro per lo svolgimento delle votazioni per il rinnovo dei Comitati degli Italiani all'Estero di cui alla legge 23 ottobre 2003, n. 286, e del Consiglio Generale degli italiani all'Estero di cui alla legge 6 novembre 1989, n. 368, nonché per introdurre in via sperimentale la modalità di espressione del voto in via digitale per lo svolgimento delle medesime votazioni.

Le elezioni dei Com.It.Es. sono disciplinate dalla legge 23 ottobre 2003, n. 286 e dal connesso Regolamento di attuazione di cui al decreto del Presidente della Repubblica 29 dicembre 2003, n. 395. La procedura elettorale è stata poi modificata dal decreto-legge 4 agosto 2014, n. 109, convertito con modificazioni dalla Legge 1° ottobre 2014, n. 141. Tutte le fasi dell'esercizio elettorale per il rinnovo dei Comitati degli Italiani all'Estero avvengono sotto la competenza del MAECI e sono gestite dalle Sedi della rete diplomatico-consolare. L'espressione di voto da parte dell'elettore avviene per corrispondenza, previa registrazione – detta "opzione di voto" – da far pervenire alla sede consolare di riferimento almeno 30 giorni prima delle elezioni, per confermare la propria volontà di votare e quindi di ricevere il plico elettorale.

In ottemperanza alla disposizione normativa sopra citata, questa Amministrazione ha avviato fin dalle prime settimane del 2021 un intenso lavoro preparatorio per realizzare una sperimentazione del voto digitale in occasione delle elezioni dei Com.It.Es., tenutesi il 3 dicembre 2021, stabilendo che la sperimentazione del voto elettronico sarebbe avvenuta parallelamente alle tradizionali operazioni elettorali in cartaceo per corrispondenza, avrebbe riguardato un novero ristretto di Sedi consolari e non sarebbe stata produttiva di effetti giuridici (il conteggio dei voti elettronici non sarebbe rilevato a fini ufficiali), rispondendo dunque a un fine puramente conoscitivo e analitico. L'assenza, infatti, di un "Polo Strategico Nazionale" su cui poter ospitare l'infrastruttura *cloud* del voto elettronico con le necessarie garanzie di sicurezza e di tutela della riservatezza dei dati, e la mancanza di una consolidata esperienza a livello internazionale in materia di *internet voting* hanno suggerito un approccio mirato alla cautela e all'aderenza al principio di graduale introduzione di tecnologie di voto elettronico. A oggi, infatti, i sistemi di voto elettronico sperimentati anche in altri Paesi europei non sempre hanno dato prova di sufficiente affidabilità e trasparenza, tanto che alcuni Paesi hanno finito per rinunciare per ora alla loro introduzione per i problemi emersi tanto sotto il profilo tecnico quanto giuridico.

Su tali basi, si è potuta realizzare una vera e propria "simulazione" atta a verificare importanti e delicati aspetti sulla futura percorribilità del voto elettronico, in particolare a tutela dei principi costituzionali di personalità, eguaglianza, libertà e segretezza del voto. Il lavoro di questa Amministrazione, oltre a tener conto delle raccomandazioni del Consiglio d'Europa, si è ispirato alle determinazioni dell'apposita Commissione interministeriale presieduta dal Ministero dell'Interno, con la partecipazione delle amministrazioni coinvolte nel voto tra cui il MAECI, e costituita con l'obiettivo di individuare delle Linee guida per il voto elettronico, in attuazione dell'articolo 1, comma 627, della Legge 27 dicembre 2019, n. 160, recante il bilancio di previsione dello Stato per l'anno finanziario 2020 e bilancio pluriennale per il triennio 2020-2022. Le suddette Linee guida sono state adottate con Decreto del Ministero dell'Interno di concerto con il Ministero dell'Innovazione il 9 luglio 2021.

Questa Amministrazione si è dovuta quindi confrontare con una sfida senza precedenti in Italia e con limitato tempo a disposizione. Il portale "IOvoto" ha visto la luce solo a seguito di un'intensa attività preliminare di analisi, con particolare attenzione agli aspetti tecnici, normativi e di processo che sono di innegabile delicatezza e complessità, quali, a titolo esemplificativo, gli aspetti dell'identificazione dell'elettore, della trasmissione e della conservazione del voto, dell'infrastruttura informatica, dell'interoperabilità tra le piattaforme interessate, del corretto computo dei voti, dell'estrazione dei dati e dell'assistenza all'utenza.

Le elezioni dei Com.It.Es. hanno consentito di sperimentare per la prima volta le procedure di voto digitale in undici Comitati appartenenti a nove Sedi diplomatico-consolari: Berlino, Monaco di Baviera (per i Comitati di Monaco di Baviera e Norimberga), Marsiglia, Londra (per i Comitati di Londra e Manchester), L'Aja, Houston, San Paolo, Tel Aviv e Johannesburg. Le sedi sono state individuate sulla base di alcuni criteri concordati: la grandezza della collettività, il livello di digitalizzazione nel Paese, il tasso di cittadini residenti registrati sul portale dei servizi consolari Fast It, la percentuale di residenti dotati di codice fiscale validato dall'Agenzia delle Entrate e la presenza di un fuso orario compatibile con l'assistenza centralizzata.
Durante la finestra temporale compresa fra il 24 novembre il 3 dicembre (ovvero nei dieci giorni antecedenti la tenuta delle elezioni) tutti gli elettori che avevano fatto richiesta di iscrizione negli elenchi elettorali per il tramite del portale consolare "Fast It" sono stati abilitati alla piattaforma "IOvoto", potendo così votare anche in via digitale autenticandosi con credenziali SPID di II livello. Il totale degli elettori abilitati sulla piattaforma è stato di 7756 "optanti digitali"; di questi, 1220 erano dotati di SPID di II livello (requisito necessario per partecipare alla sperimentazione). Hanno infine votato in 672 "votanti digitali" dimostrando proporzionalmente una propensione alla partecipazione al voto maggiore rispetto al tradizionale voto per corrispondenza.
La sperimentazione è stata disciplinata dal decreto ministeriale MAECI n. 4112/2578 del 22 novembre 2021.

1 INTRODUZIONE AL DOCUMENTO

Il presente documento è stato redatto secondo quanto previsto dall'art.6, co. 2, del D.M. 4112/2578 del 22 novembre 2021, per valutare gli esisti dell'introduzione in via sperimentale di modalità di espressione del voto in via digitale in occasione delle elezioni per il rinnovo dei Comitati degli Italiani all'Estero (Com.It.Es.), tenutesi il 3 dicembre 2021.
Come indicato nelle Premesse, sono stati coinvolti nella sperimentazione gli undici Comitati di nove sedi diplomatico-consolari: Berlino, Houston, Johannesburg, Londra, Manchester, L'Aja, Marsiglia, Monaco di Baviera, Norimberga, San Paolo e Tel Aviv.
La sperimentazione è stata riservata agli elettori delle sedi selezionate che hanno presentato richiesta di iscrizione nell'elenco degli elettori per le elezioni dei Com.It.Es. per il tramite del portale Fast It, al fine di accrescere le garanzie di correttezza, completezza e attualità dei dati anagrafici e di contatto dell'elettore.
Alcune scelte dell'implementazione della soluzione tecnica sono state adeguate al carattere sperimentale e privo di valore della sperimentazione ed è stata indicata di volta in volta la soluzione tecnica completa che dovrebbe essere adottata nel caso in cui si decidesse di rendere giuridicamente valida tale modalità di raccolta dei voti.

1.1 TERMINI, DEFINIZIONI E ACRONIMI

Di seguito sono elencati tutti gli acronimi e le abbreviazioni adottati nel presente documento.

#	Termine	Definizione
1	MAECI	Ministero degli Affari Esteri e della Cooperazione Internazionale
2	DGIT	Direzione Generale per gli Italiani all'Estero e le politiche migratorie
3	DGAI	Direzione Generale per l'amministrazione, l'informatica e le comunicazioni
4	COM.IT.ES.	Comitato degli Italiani all'Estero
5	Fast It	Portale dei servizi consolari online
6	CF	Codice Fiscale
7	IdP	Identity Provider SPID

Tabella 1 - Termini e Acronimi

2 INTRODUZIONE AL PORTALE VOTO ELETTRONICO

Il Portale Voto Elettronico è un portale WEB costituito da:

- Front Office "iovoto.esteri.it": sito per gli elettori che possono esprimere il proprio voto online, identificandosi con SPID di II livello;
- Back Office "elettorale.esteri.it": sito per gli operatori designati mediante il quale si effettua lo scrutinio elettronico dei voti; accesso tramite SPID di II livello.

Inoltre, si sono rese necessarie alcune applicazioni specifiche per le operazioni di configurazione riguardanti:

- caricamento delle liste e dei simboli;
- caricamento dei candidati per ciascuna lista;
- caricamento dell'elenco degli elettori ammessi al voto.

Trattandosi queste ultime di operazioni molto onerose in termini di risorse e di tempo, l'interfaccia utente ad uso esclusivo del personale tecnico è molto semplificata ed in caso di elezione su vasta scala dovrà subire una reingegnerizzazione per ottenere maggiore efficienza ed usabilità.

La platea di elettori ammessi alla sperimentazione è stata ristretta agli elettori dei Com.It.Es. sperimentanti che hanno fatto pervenire l'opzione di voto alla propria sede consolare di competenza entro 30 giorni dalla data prevista per il voto (quindi entro il 3.11.2021) mediante Fast It.

A seguito dell'accesso di un utente al portale IOvoto, quest'ultimo verifica se l'utente è abilitato a partecipare alla sperimentazione, in tal caso consente di procedere con il voto.

Questa verifica è effettuata cercando il CF dell'elettore inviato dall'IdP SPID fra quelli presenti nell'elenco elettori; se il CF non è presente, al connazionale viene richiesto l'inserimento del proprio Codice Elettore, recuperabile dalla propria area personale di Fast It oppure sul plico cartaceo ricevuto per posta per partecipare al voto tradizionale cartaceo. Se fallisce anche questa seconda modalità di ricerca, l'utente non viene considerato come elettore e dunque non è ammesso al voto.

Se l'utente viene riconosciuto come avente diritto, visualizza la schermata iniziale del Com.It.Es. di competenza, poi viene condotto all'interno della cabina elettorale virtuale dove può prendere visione del manifesto elettorale e visualizzare il Codice di Convalida attribuitogli dal portale. Questo codice è univoco, personale e funzionale all'espressione pseudonimizzata del voto (operazione che consente di disgiungere i dati dell'elettore dalle sue scelte elettorali).

L'elettore può esprimere il proprio voto selezionando una delle liste indicate o selezionare, in alternativa, la voce "scheda bianca" per non votare per alcuna lista. Nel primo caso, l'iter di voto prosegue con l'espressione dei voti di preferenza, per un totale massimo di un terzo dei candidati da eleggere. In un successivo momento, l'elettore potrà accedere nuovamente al portale, in nessun caso potrà esprimere di nuovo il proprio voto, ma potrà scaricare la ricevuta elettronica che attesta l'avvenuta votazione.

3 CRITICITÀ AFFRONTATE E PROPOSTE DI SOLUZIONE

3.1 INFRASTRUTTURA

Il portale IOvoto consiste in due applicazioni fisicamente distinte, **Applicazione1** e **Applicazione 2.** Entrambi gli applicativi sono aperti al pubblico e gestiscono le operazioni effettuate da utenti esterni (autenticazione, espressione del voto online). Il processo si svolge in due applicativi separati per garantire la segretezza del processo di voto, ma vengono esposti all'utente come un'unica applicazione.

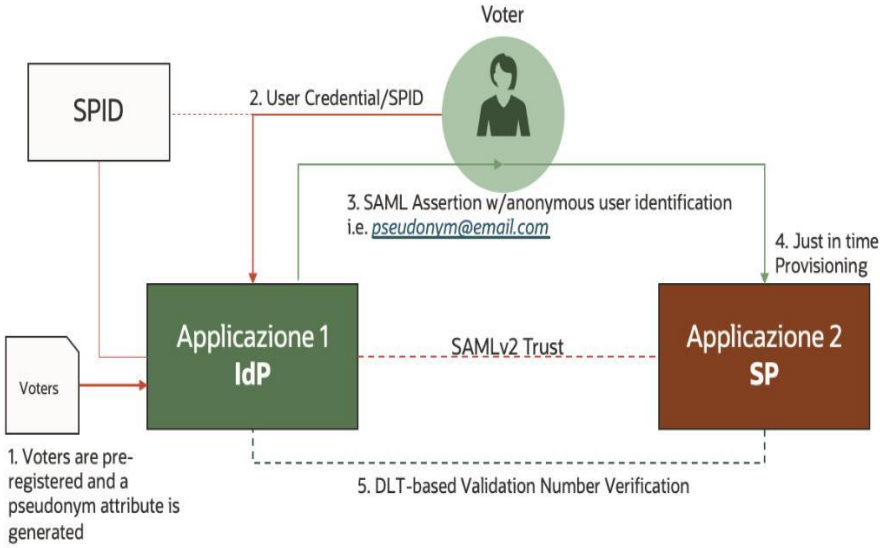

Figura 1 - Architettura portale IoVoto

Di seguito è schematizzata l'architettura realizzata in cloud:

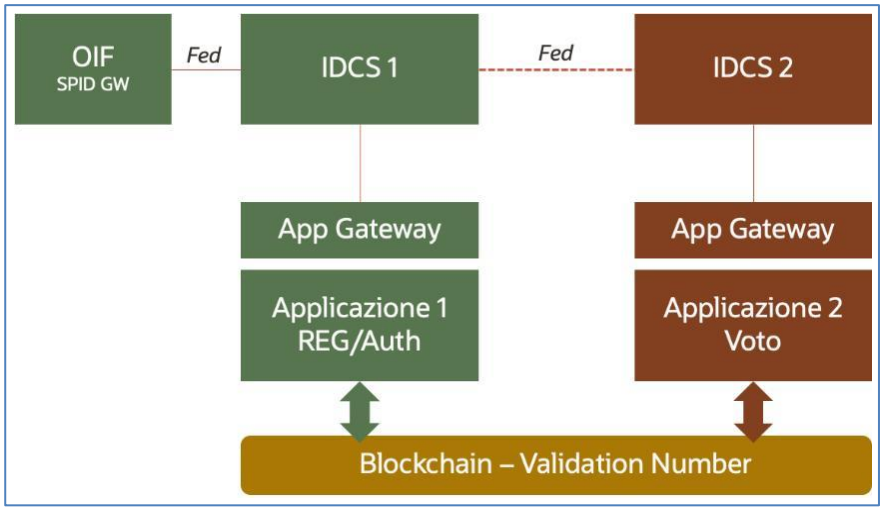

Figura 2 - Architettura cloud

Le due applicazioni hanno in comune la blockchain mediante la quale viene registrato il voto espresso attraverso la pseudonimizzazione e la separazione degli ambienti.

3.2 CRITICITÀ DELL'INFRASTRUTTURA

Per ospitare l'intera infrastruttura è stata utilizzata l'infrastruttura **cloud Oracle** con il vincolo di dislocare gli ambienti di test e di produzione nel datacenter di Francoforte in Germania, su territorio europeo.
Questa scelta è stata il miglior compromesso individuato fra la tutela della privacy dei dati degli elettori e le garanzie di gestione tecnica avanzata fornite da personale Oracle con il quale era stato stipulato il contratto di acquisto di licenze, con offerta migliorativa di servizi complementari per la realizzazione di blockchain e configurazione del sistema IDCS (IDentity Cloud Service).
Come segnalato anche nelle interlocuzioni con il Garante della Privacy, questa non potrà essere la scelta nel caso in cui si decidesse di applicare questa modalità di voto elettronico ad una platea più estesa (ad esempio la totalità degli elettori).

Nell'implementazione di una modalità di voto elettronico con valore legale, bisognerà puntare necessariamente all'uso del cloud del nascente Polo Strategico Nazionale, con garanzie di sicurezza sul trattamento di dati personali certamente superiori rispetto a quanto è stato realizzato sul cloud Oracle.

Lo sforzo notevole è stato quello di inserire tutti i dati in maniera cifrata e non intelligibili da parte dei consulenti e dei collaboratori, se non previo accordo con personale MAECI che deteneva le chiavi di cifratura.
Si segnala che anche questa modalità di trattamento pone seri interrogativi riguardo la gestione delle chiavi di cifratura da parte di un'unica persona, che potrebbe in ogni caso essere ricattabile o costretta ad operare a danno della riservatezza dei dati o della segretezza del voto, o addirittura modificando l'esito del voto. Anche nel caso in cui tali eventi non si verificassero si segnala che il funzionamento del portale resta a disposizione di numero limitato di tecnici specializzati che hanno contribuito alla sua realizzazione. Al contrario del voto cartaceo, il cui funzionamento è noto a tutte le persone coinvolte (scrutatori, capi lista ecc.) il fatto che il funzionamento della piattaforma sia limitato a pochi esperti può dare adito a contestazioni sulla possibilità di brogli nell'uso della piattaforma. Anche nel caso in cui nessuna manipolazione del voto abbia avuto luogo, la mancanza di una verifica diffusa sulla correttezza del risultato elettorale può far venir meno la fiducia nel sistema. Per fare un esempio, un'accusa di brogli da parte di una lista perdente potrebbe comportare l'annullamento delle elezioni anche ove nessun broglio abbia avuto luogo, semplicemente minando la fiducia nel sistema.

Inoltre è opportuno segnalare che mentre il voto cartaceo è compartimentato per seggio (nel caso di specie per singolo Com.It.Es.), con il voto elettronico i risultati sono aggregati a livello centrale. Un attacco informatico che avesse successo nel violare questa infrastruttura, anche se rilevato dalla blockchain (vedasi paragrafo 3.3) comprometterebbe l'intero processo elettorale, che andrebbe ripetuto. È possibile, anche se più costoso in termini di tempo e risorse, nel caso specifico dei Com.It.Es. studiare opzioni che isolino in parti diverse dell'infrastruttura ogni risultato dagli altri nel caso di attacchi informatici, essendo ogni singolo Com.It.Es. indipendente dall'altro.

3.3 CRITICITÀ BLOCKCHAIN

La parte di configurazione della blockchain è stata demandata ai consulenti delle ditte incaricate perché richiedeva delle conoscenze specialistiche e di dettaglio relative a tale ambiente e non acquisibili da personale interno, visti i tempi molto ristretti in cui ci si è trovati ad operare.
Questa configurazione dell'ambiente riveste un ruolo cruciale nella sicurezza della soluzione tecnica realizzata, per cui è necessario rendere autonomo il personale tecnico interno al MAECI in maniera da poter realizzare e configurare la blockchain o poter verificare la correttezza dell'operato dei consulenti. Per agire su questa criticità la soluzione è la formazione specialistica di risorse interne su tale materia.
Va approfondita anche in questo ambito la gestione delle credenziali di accesso di coloro che possono agire sui dati della blockchain.

Legate a questo argomento ci sono anche alcune criticità relative alle operazioni di popolamento del portale:
1) creazione e caricamento dell'elenco elettori con aggiunta dello pseudonimo;
2) creazione e caricamento delle liste, dei simboli e dei candidati.

Per quanto riguarda le operazioni indicate al punto 1, queste hanno riguardato i seguenti elettori optanti su Fast It:

Com.It.Es.	Optanti Fast It
BERLINO	578
HOUSTON	201
JOHANNESBURG	44
L'AJA	793
LONDRA	2.418
MANCHESTER	663
MARSIGLIA	601
MONACO DI BAVIERA	428
NORIMBERGA	36
SAN PAOLO	1.935
TEL AVIV	59
	Tot. 7.756

Tabella 2 - Optanti delle sedi sperimentanti

Le operazioni di creazione dell'elenco degli elettori che partecipano al voto elettronico si basano sulla raccolta di alcuni dati dell'elenco elettori (NOME | COGNOME | SESSO | DATADINASCITA | LUOGODINASCITA | CODICEFISCALE | CODICEELETTORE | COM.IT.ES | PSEUDONIMO) in formato csv (Comma-Separated Values, valori separati da virgola, non è altro che un file di testo, che utilizza le virgole per separare i dati contenuti all'interno delle singole celle di una tabella; nel caso specifico è stato utilizzato il carattere "|" come separatore).
Questo elenco viene caricato mediante un applicativo di servizio all'interno del ledger "ELETTORI" per consentire l'identificazione degli aventi diritto che si identificano mediante SPID di II livello. L'attività implica tempi di esecuzione elevatissimi che possono essere ridotti solo in parte con l'esecuzione parallela di più istanze contemporanee, poiché comporta l'utilizzo di notevoli risorse di calcolo (per 7756 elettori sono state necessarie circa 6 ore per il caricamento in blockchain).
Poiché in fase di raccolta dei dati, va inserito anche lo pseudonimo da associare a ciascun elettore, si è scelto di produrre un hash del codice elettore con algoritmo di cifratura AES256 con chiave a 32 caratteri. Anche questa operazione eseguita da personale interno in maniera non automatizzata, non può essere riproposta nel caso di una elezione con valore legale poiché il trattamento di elenchi più numerosi necessita di una standardizzazione dei processi, al fine di ridurre l'intervento umano per l'esecuzione di operazioni ripetitive e complesse, essendo richiesta sicurezza e certezza dell'azione, nonché maggiore celerità.
Le liste (name | imageUrl | Com.It.Es | rangoSedeCompetenza | cittaSedeCompetenza | ordine | maxSel | timeZone) ed i nominativi dei candidati di ciascuna lista (nomeCandidato | cognomeCandidato | dataNascitaCandidato | luogoNascitaCandidato | ordine| lista) sono stati esportati in formato csv per essere caricati nei ledger "LISTE" e "CANDIDATI"; associato a ciascuna lista era presente anche il nome del file del simbolo, costituito da un file immagine in formato jpeg, jpg o png. Questi dati sono stati raccolti tramite un altro portale elettorale utilizzato dagli operatori delle sedi estere che gestivano le elezioni dei singoli Com.It.Es.

Le liste ed i relativi simboli erano 27 per tutti i Com.It.Es. sperimentanti, con 443 candidati in totale.
Su queste operazioni sono necessari diversi interventi di automazione e correzione:

- poiché bisogna riprodurre lo stesso ordinamento delle liste e dei nominativi dei candidati presente all'interno del portale elettorale ed utilizzato anche nella stampa delle schede cartacee, va prevista una **modalità di estrazione dei dati automatica** e priva di interventi manuali, come invece è stato fatto in questa sperimentazione dati gli esigui numeri;
- alcune liste sono presenti su più sedi con lo stesso nome, ma all'interno del ledger delle liste il nome è un campo chiave quindi non possono essere presenti liste duplicate; per ovviare a questa criticità è necessario modificare il relativo ledger inserendo un **identificativo numerico univoco**;
- in alcuni casi i nominativi dei candidati con caratteri diacritici non sono stati caricati correttamente dalla blockchain e quindi non risultavano visibili ai primi utenti che hanno fatto accesso al portale di voto; l'errore è stato corretto in corso d'opera, con un nuovo caricamento; in prospettiva va prevista una **procedura di verifica e validazione** di liste, simboli e candidati prima dell'apertura delle operazioni di voto;
- alcuni dei simboli non erano visibili ai primi utenti che volevano esprimere il proprio voto digitale, poiché il nome del file caricato in blockchain non corrispondeva a quello utilizzato su file system; occorre prevedere una **procedura di verifica automatica** di questa corrispondenza.

3.4 CRITICITÀ SESSIONI DI COLLAUDO

Si sono svolte due sessioni di collaudo dell'intera procedura con caricamento di elettori, liste e candidati nei giorni: 02/11/2021 e 17/11/2021. Alcune problematiche sono emerse nel corso di queste sessioni e sono state prontamente corrette, ma non è mai stato collaudato un **carico di utenti abbastanza consistente**; infatti, quando è stato attivato l'ambiente di produzione (durante i giorni dedicati al voto dal 23/11/2021 al 03/12/2021), sono state eseguite operazioni sulle macchine virtuali delle applicazioni, per inserire il bilanciamento di carico e la ridondanza delle macchine stesse. Poiché le applicazioni non erano state collaudate in questa modalità, si sono verificati problemi per alcuni utenti, i quali in alcuni casi non sono riusciti ad esprimere il voto al primo tentativo ma sono stati ricontattati per farlo successivamente, in altri casi non sono riusciti a scaricare la ricevuta. Le attività non erano concordate ed hanno comportato alcuni disservizi; in caso di voto con valore legale, non è accettabile tale disservizio: eventuali modifiche alle configurazioni vanno collaudate sull'ambiente di test, prima di essere rilasciate in produzione. La problematica emersa mette in luce la necessità di notevoli investimenti al fine di garantire un'assistenza informatica 24 ore su 24 nel corso dell'evento elettorale e ulteriormente rafforzata in fase di "chiusura dei seggi". Il rischio è altrimenti, nel caso di un voto con pieno valore legale, di negare ai cittadini un diritto costituzionalmente garantito per problematiche di natura tecnica.

3.5 CRITICITÀ EMERSE A SEGUITO DEI PENETRATION TEST

L'applicazione è stata sottoposta a Penetration Test da parte di un'azienda terza rispetto all'azienda sviluppatrice, dal 02/11/2021 al 10/11/2021.
Il Penetration Test è il servizio che ha lo scopo di evidenziare le eventuali vulnerabilità e problematiche di sicurezza presenti e di indicare contromisure di tipo tecnologico, organizzativo e procedurale, in grado di eliminare le vulnerabilità e le problematiche, mitigarne gli effetti ed innalzare lo stato complessivo della sicurezza dell'intera infrastruttura tecnologica.
Le attività di Penetration Testing sono state effettuate tenendo conto delle seguenti metodologie di riferimento:

- OWASP Testing Guide
- Penetration Testing Execution Standard
- OSSTMM

L'attività di Security Testing ha evidenziato una Overall Cyber Risk Level pari a MEDIO.
Il calcolo dell'esposizione al rischio Cyber complessivo è dato dalla formula: Overall Cyber Risk Level = Likelihood Factors * Impact Factors.

Probabilità "MEDIA": la probabilità dà un'indicazione su quanto debba considerarsi possibile un attacco nei confronti del target e viene calcolata sulla base di diversi fattori, tra cui quante competenze tecniche debbano avere gli attaccanti per portare a termine l'attacco con successo, di quanto il target sia appetibile, della facilità di scoperta delle vulnerabilità e così via.
Impatto "MEDIO": la valutazione degli impatti cerca di dare una stima qualitativa delle conseguenze che un attacco potrebbe avere. Tale valutazione viene alimentata da diversi fattori, che cercano di tenere conto di diverse dimensioni, tra le quali: il possibile danno di immagine, il danno finanziario, la perdita di riservatezza, integrità e disponibilità dei dati.

Le informazioni pubbliche rilevate fanno riferimento a un totale di 26 Vulnerabilità sul target. Nello specifico si segnala che sono state individuate:

- 23 vulnerabilità con livello di criticità MEDIO;
- 3 vulnerabilità con livello di criticità ALTO.

La distribuzione, per percentuale di rischio, delle vulnerabilità identificate dall'attività è rappresentata dal grafico:

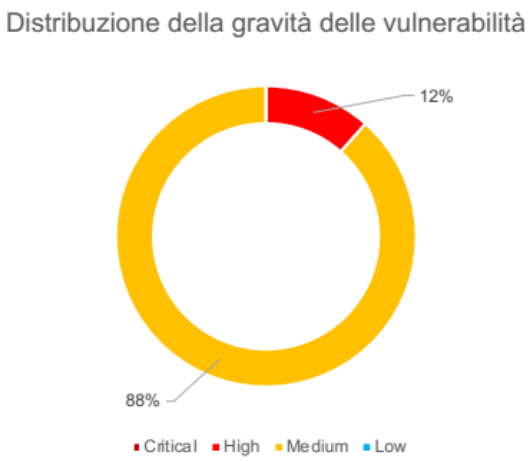

Figura 3 - Distribuzione della gravità delle vulnerabilità

Si riporta di seguito il sommario delle minacce e delle vulnerabilità riscontrate:

Vulnerabilità	Assets	Sintesi remediation	CVSSv3.1
Esposizione di informazioni [3]	Codice sorgente	Cambiare le credenziali di accesso al server IDCS https://comitestest-elettoricomites-fra.blockchain.ocp.oraclecloud.com:7443 Limitare gli accessi degli elettori alle sole risorse necessarie ai fini della votazione. Cambiare il nome del DataBase applicativo	**8.8 - High**
	https://idcs-f10c63c1d7aa48249bdc88af20059935.identity.oraclecloud.com/ui/v1/myconsole?root=my-info		
	Github Commit del codice sorgente		
Security headers mancanti [12]	https://iovoto.esteri.it/	Aggiungere nel file di configurazione del Web Server utilizzato, tutti gli headers di sicurezza.	**6.3 – Medium**
	https://iovotocomites.esteri.it/		
Flag di sicurezza mancanti per cookie di sessione [7]	iovoto.esteri.it	Tutti i cookie di sessione devono essere accompagnati dal flag "Secure".	**5.3 – Medium**
	iovotocomites.it		
	elettorale.esteri.it		
Directory Listing	https://iovotocomites.esteri.it/	Cambiare le configurazioni del web server	**4.6 – Medium**
Configurazione SSL/TLS Insicura [3]	https://iovotocomites.esteri.it	Effettuare l'hardening della configurazione SSL/TLS.	**0.0 – Info**
	https://elettorale.esteri.it		
	https://iovoto.esteri.it		

Tabella 3 - Vulnerabilità

Tutte le segnalazioni sono state ricevute una settimana prima dell'apertura dell'ambiente di produzione per cui, pur ritenendo utili e necessari gli interventi suggeriti, non è stato possibile modificare di conseguenza le configurazioni né le applicazioni per ridurre il rischio.
Nel momento in cui si decidesse di adottare questa soluzione di voto elettronico, è **assolutamente indispensabile adeguare preventivamente l'infrastruttura ed il software** come da indicazioni ricevute. È tuttavia opportuno segnalare che pur adottando ogni utile accorgimento al fine di garantire il margine di sicurezza più alto possibile, a livello informatico non è possibile garantire una sicurezza del 100%. Tenuto conto dell'interesse che attori statuali o non statuali potrebbero avere nel portare attacchi informatici contro la piattaforma nel caso di un uso della stessa con pieno valore legale, nell'eventualità in cui si decidesse di procedere in tal senso, bisognerebbe accettare il rischio di attacchi informatici che, come già indicato in precedenza, comporterebbero l'annullamento delle elezioni e la ripetizione delle stesse, con conseguente danno sia per l'erario che per l'immagine della PA.

3.6 CRITICITÀ SULLA PUBBLICAZIONE DEL CODICE SORGENTE SU GITHUB

Per errore, nella pubblicazione dei sorgenti delle applicazioni di voto, in una porzione di codice commentata, sono state rinvenute in chiaro le credenziali di accesso alla dashboard di amministrazione della blockchain dell'ambiente di test e di conseguenza alle rest API per l'interfacciamento con la stessa e al servizio IDCS (contenente i dati personali degli elettori). Ciò non ha inficiato in alcun modo le operazioni di

voto né nelle sessioni di collaudo né nella sessione di voto della sperimentazione, ma ha consentito alla ditta che svolgeva i test di acquisire ulteriori informazioni sull'infrastruttura e sulle sue vulnerabilità.

3.7 CRITICITÀ SULLA SEGRETEZZA DEL VOTO

La **segretezza** del voto risulta un requisito necessario per ogni sistema di voto, compreso il voto elettronico. Nessun attore dovrebbe essere in grado di ricostruire l'informazione del votante e della lista e candidato a cui egli ha affidato il proprio voto. Sul portale IOvoto, un attore malevolo con accesso all'IDCS e alla Blockchain potrebbe essere in grado di recuperare l'associazione votante-candidati, invalidando il principio di segretezza del voto.
Questa possibilità si può verificare se gli amministratori dei due sistemi si mettono d'accordo, ovvero nel caso in cui un attore malevolo interno, che nei riguardi dei risultati di una votazione dovesse trovarsi in una posizione di conflitto di interessi, potrebbe tracciare il risultato della votazione.
Il problema emerge poiché le query, comprensive di parametri, sono visibili nei log delle transactions su Oracle Blockchain Platform Cloud Console agli amministratori della Blockchain.
L'intervento per mitigare questa criticità è sicuramente complesso data la natura del contesto in cui il voto viene effettuato da una posizione remota e attraverso un dispositivo personale. A parziale mitigazione, si dovrà disaccoppiare in qualsiasi punto del flusso di votazione l'associazione tra lo pseudonimo e i candidati votati. Inoltre, ogni forma di tracciamento delle attività (logging) dovrà essere il più possibile generico in ogni punto dell'architettura dove si faccia riferimento alla votazione espressa dall'utente.
Inoltre, per garantire maggiormente la segretezza del voto rispetto a ingerenze esterne ma di natura non informatica e per evitare il voto di scambio (si pensi a un candidato che chiede di visualizzare il voto elettronico dei propri elettori in cambio di favori e regalie, oppure di un datore di lavoro che chiede ai propri dipendenti di votare per lui, pena il licenziamento) si deve garantire all'elettore la possibilità di poter votare in più di un'occasione fino alla "chiusura dei seggi". Il sistema deve chiaramente registrare come voto valido solo l'ultimo voto espresso (altrimenti si avrebbero voti multipli per il medesimo elettore). Questo sistema ridurrebbe notevolmente eventuali episodi di voto di scambio, in quanto si deve essere in grado di controllare l'elettore proprio nei minuti che precedono la chiusura dei seggi, cosa che risulta impossibile su grandi numeri. Tuttavia l'avvio di una simile funzione comporterebbe una notevole pressione sull'infrastruttura informatica nelle ore prima della "chiusura dei seggi". Sono pertanto necessari notevoli investimenti al fine di garantire una sua resistenza a qualsiasi carico di lavoro come già specificato al punto 3.4.

3.8 CRITICITÀ SULL'INTEGRITÀ E SULLA VERIFICABILITÀ DEL VOTO

L'applicazione non dispone di meccanismi in grado di dare garanzia all'elettore che il proprio voto sia esattamente quello da lui immesso. In un sistema di voto il cittadino dovrebbe avere la possibilità di verificare che il proprio voto sia custodito in modo integro e sia quindi valutato correttamente. In un sistema di voto tradizionale, il cittadino è tutelato dalla presenza delle componenti del seggio elettorale e delle forze dell'ordine. Nel sistema IOvoto, invece, non è prevista la verifica dell'integrità del proprio voto. Il cittadino, dunque, deve necessariamente "fidarsi" del processo e dei mezzi tecnici messi a disposizione. Un attore malevolo interno, che nei riguardi dei risultati di una votazione dovesse trovarsi in una posizione di conflitto di interessi, potrebbe alterare in modo tecnico il risultato della votazione, senza alcuna possibilità di verifica.
In particolare, l'elettore dovrebbe porre la propria fiducia nei fornitori privati degli enti governativi e nelle infrastrutture di rete utilizzate per il voto in un contesto in cui tali enti potrebbero essere in una posizione di conflitto di interessi nei riguardi del risultato del voto stesso.
Dal punto di vista dell'**integrità** del voto, è fondamentale che l'informazione non sia modificata prima di essere inserita nella blockchain. Ciò può dipendere da molti fattori di cui si potrebbe non avere il controllo diretto.
Per quanto riguarda la **verificabilità**, un sistema di blockchain decentralizzato potrebbe agevolarla permettendo a ciascun elettore la verifica del proprio voto attraverso, ad esempio, tecniche crittografiche (encryption e/o verifica di una firma digitale). Anche in quest'ultimo caso, si dovrà fare affidamento sull'integrità dei sistemi utilizzati dall'utente per la verifica stessa.
A parziale mitigazione di questa criticità è stata prevista la pubblicazione del codice sorgente delle applicazioni di voto, ivi compresa la piattaforma blockchain. Per questa sperimentazione è stata invece utilizzata una blockchain proprietaria.
Si vedano a riguardo i dubbi già sollevati nel paragrafo 3.2.

3.9 CRITICITÀ SULLE OPERAZIONI DI SPOGLIO

Un sistema di voto dovrebbe garantire il fatto che i risultati ufficiali possano essere disponibili, e quindi potenzialmente divulgati, solo al termine della votazione allo scopo di non influenzare la votazione in corso. Un attore, con capacità di accesso in lettura alla Blockchain, potrebbe costantemente monitorare l'andamento della votazione con possibilità, quindi, di prendere azioni di comunicazione correttive per favorire l'uno o l'altro candidato.

Nel sistema IOvoto sono assenti restrizioni tecniche alla lettura della Blockchain da parte ad esempio di un attore insider. Inoltre, un elettore non avrebbe modo di accertarsi che questo non venga realmente fatto.
Nel portale dello spoglio elettronico dei Com.It.Es. il calcolo dei seggi da attribuire a ciascuna lista si basa sul numero di voti riportati (a prescindere dall'indicazione di uno o più candidati). Sull'analisi di questo processo le indicazioni non sono state recepite correttamente e quindi l'algoritmo di attribuzione andrà rivisto e perfezionato.
Bisognerà analizzare con maggior dettaglio anche i profili di autorizzazione che si vogliono concedere a coloro che hanno accesso all'applicazione di spoglio, per stabilire se è necessario riprodurre un seggio con i vari componenti previsti nel voto tradizionale cartaceo o se le operazioni possono essere semplificate tenendo conto del fatto che buona parte del lavoro viene svolto in automatico dal portale stesso.
Si vedano a riguardo i dubbi già sollevati nel paragrafo 3.2.

3.10 CRITICITÀ SULLA DISPONIBILITÀ DEL SERVIZIO

Un sistema di voto dovrebbe garantire a tutti gli elettori di poter esercitare il diritto di voto in ogni caso.
Un attacco informatico, da parte di un attore malevolo, potrebbe produrre un malfunzionamento dei sistemi in grado di causare un disservizio; ciò potrebbe impedire il processo di votazione (Denial of Service o Distributed Denial of Service). Il disservizio potrebbe avere origine anche localmente su qualsiasi punto dell'infrastruttura di voto. In queste condizioni, i risultati delle elezioni potrebbero non risultare effettivi.
Il rischio di un disservizio, sia che avvenga sui votanti che sull'applicativo, comprometterebbe il risultato delle elezioni in quanto ci sarebbe un impedimento, per una porzione di elettori, di esprimere il proprio voto.
In un sistema di voto elettronico che fa anche affidamento su un'infrastruttura non direttamente controllabile, come il device dell'elettore e la sua connessione a internet, potrebbe essere complesso assicurarsi che ogni componente del sistema di voto sia sempre disponibile.
Si vedano a riguardo anche i dubbi già sollevati al paragrafo 3.5.

3.11 CRITICITÀ SULL'HELPDESK

In questa sperimentazione non è stato previsto un servizio di assistenza agli elettori. Data la natura sperimentale di questa elezione è stato reso disponibile un indirizzo e-mail dedicato ad eventuali richieste di assistenza o per le segnalazioni di malfunzionamenti. Non avendo a disposizione personale da dedicare h24 a tale attività, l'assistenza è stata svolta in maniera asincrona, compatibilmente con gli altri impegni. Le richieste non sono state numerose e per la maggior parte legate a malfunzionamenti del dispositivo e/o del browser utilizzato. Si vedano a riguardo i dubbi già sollevati nel paragrafo 3.4.

3.12 CRITICITÀ SUI FORNITORI

La sicurezza del sistema IOvoto dipende anche dalla sicurezza dei fornitori che l'hanno realizzata e da quella dei fornitori dei servizi coinvolti per la sua operatività. Un attore malevolo (di tipo sia statuale che non) potrebbe compromettere uno dei fornitori coinvolti al fine di ottenere informazioni (ed esempio credenziali di accesso dell'istanza di Oracle Blockchain Platform) che potrebbero consentire di accedere ad esempio alle funzionalità di gestione della Blockchain e potenzialmente influenzare i risultati delle votazioni.
Un altro possibile scenario, collegato al precedente, potrebbe ad esempio consentire agli attori malevoli di carpire le credenziali dell'utenza Github con il codice sorgente dell'applicativo ed effettuare tentativi di tampering dello stesso effettuando eventuali commit allo scopo di modificare l'applicazione in modo malevolo.
Per mitigare questi rischi, a valle dei test, è stato consigliato quanto segue:
• Realizzare di un processo di Secure Software Development Lifecycle;
• Creare processi e linee guida per lo sviluppo di codice sicuro da condividere con i fornitori per la realizzazione o manutenzione delle applicazioni;
• Effettuare attività periodiche di Security Assessment e Risk Assessment;
• Rimuovere/modificare tutti i riferimenti (commenti, codice di test, pseudonimi, email) dal repository che possano avvantaggiare ad esempio azioni di social engineering;
• Assicurarsi di modificare e tenere strettamente riservate tutte le informazioni sensibili utilizzate come chiavi private, credenziali, URL di produzione e altri secret;
• Assicurarsi che sia utilizzata, da parte di tutti i fornitori, l'autenticazione a multifattore.
Alcune di queste raccomandazioni sono già in atto presso la nostra Amministrazione e presso i fornitori, per altre è in corso la realizzazione di un progetto generale di messa in sicurezza del codice e delle applicazioni MAECI.

4 CONCLUSIONI

4.1 SUCCESSO DELL'OPZIONE SU FAST IT

L'opzione di voto è stata espressa per la prima volta anche tramite il portale dei servizi consolari Fast It e questa opportunità ha riscosso un grande successo poiché la percentuale delle opzioni pervenute con questa modalità innovativa è stata pari al 19% di tutte quelle pervenute (anche con le altre modalità: di persona in consolato, via mail, ecc.)
Nel grafico seguente sono riportati gli optanti delle sedi sperimentanti: tutti gli optanti (grigio), gli optanti tramite Fast It (arancione) e i partecipanti alla sperimentazione (azzurro).
La platea di optanti più giovani (20-29 e 30-39), con maggiore propensione all'uso della tecnologia, è quella che ha partecipato maggiormente alla sperimentazione.

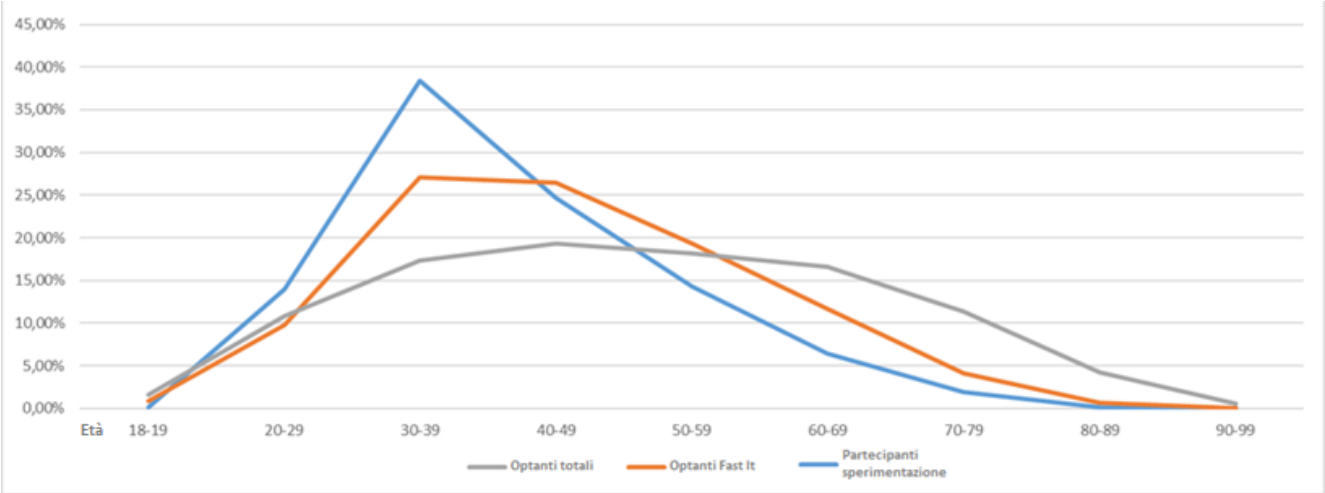

Figura 4 - Optanti per fasce di età

4.2 SUCCESSO DELLA MODALITÀ DI VOTO:

La percentuale media di votanti rispetto al numero degli elettori del portale IOVoto è di poco inferiore all'11%; questo dato è molto confortante considerando che si trattava solo di una sperimentazione e che l'ostacolo principale per i cittadini residenti all'estero è il possesso e l'utilizzo di SPID di II livello.
Questa modalità di voto da remoto, con utilizzo di strumenti elettronici personali e del sistema di identificazione SPID, ha riscosso un grande successo presso gli italiani residenti all'estero, soprattutto considerando che sono state rappresentate varie tipologie di comunità dislocate in luoghi diversi in quasi tutti i continenti.
Ovviamente le varie criticità evidenziate non possono essere eliminate, ma sicuramente molte di esse possono essere mitigate con interventi abbastanza semplici ed immediati. Le criticità relative al modello organizzativo che sottende alla distribuzione delle responsabilità e quindi delle credenziali di accesso ai tenant ed alle blockchain, possono essere mitigate con la gestione distribuita di chiavi o permessi di accesso su più attori, eventualmente di amministrazioni diverse.
Inoltre, vanno fatte alcune considerazioni sulle scelte progettuali adottate nella realizzazione del portale IOvoto, distinguendo due ambiti principali:

1. **Infrastruttura**: l'utilizzo dei servizi cloud di Oracle ha comportato la realizzazione di chain code strettamente legati alla tipologia di blockchain utilizzata in questo contesto; per tale motivo e considerando i tempi ristrettissimi a disposizione, è stato necessario coinvolgere consulenti Oracle nella realizzazione. Di conseguenza, le competenze specialistiche su tale materia sono rimaste appannaggio di quel personale e dovendo nuovamente configurare un ambiente simile si ritiene di non avere internamente le conoscenze sufficienti; sarebbe opportuno prevedere dei corsi per il personale tecnico dell'Amministrazione. Per le questioni legate al trattamento dei dati personali dei cittadini italiani, si rende necessario valutare l'utilizzo in futuro di infrastrutture di altre PA o ambienti cloud di aziende italiane.
2. **Applicazioni**: le applicazioni di voto e di spoglio sono state disegnate e realizzate sullo specifico modello di espressione del voto e di raccolta dei dati per l'elezione dei Com.It.Es. (Legge 286/2003, DPR 395/2003 DL 109/2014, art. 10) poiché i tempi molto ristretti di realizzazione non consentivano il disegno di applicazioni parametriche e personalizzabili per i vari tipi di votazioni. Sarebbe opportuno

concordare con il Ministero dell'Interno, che si occupa di coordinare le operazioni di gestione di tutti gli altri tipi di elezioni, le modalità per rendere più flessibile l'applicazione di raccolta dei voti e quella di spoglio, in maniera da renderle adattabili a tutte le esigenze.

4.3 CONCLUSIONI DELL'ANALISI TECNICA

Sulla base dell'analisi delle varie criticità rilevate, considerando che alcune di esse sono risolvibili con ulteriori interventi tecnici, è possibile affermare che l'utilizzo del voto elettronico a distanza è **attuabile per l'elezione dei Com.It.Es.**, perché anche in caso di attacchi o manomissioni non si ravvede un livello di rischio tale da inficiare la gestione di questo specifico evento elettorale, tenuto conto della sua natura diffusa, in modo analogo a quanto avviene per i Comuni in Italia.
Da un punto di vista tecnico, ad oggi andrebbe **invece ulteriormente approfondita l'estensione della sperimentazione ad altre tipologie di eventi elettorali** (elezioni politiche, referendum, elezioni europee). Si ritiene infatti fondamentale verificare le risorse necessarie per garantire l'affidabilità del sistema e la sua sicurezza.