ID TECHNOLOGY
PROPOSTA PER LA FORNITURA DI UN SERVIZI DI VOTO ELETTRONICO (E-VOTING)

Allegato tecnico breve ELIGO

Sommario

1. ABSTRACT DI PROGETTO

1.1. Obbiettivi e premessa del progetto

L'obbiettivo del progetto è applicare nuove tecnologie e processi di voto più moderni ed adatti al mondo digitale attuale. Tutto questo senza in nessun modo prescindere dalle caratteristiche di sicurezza, anonimato, univocità intrinseche al diritto di voto.

I fini ultimi del progetto sono:

- Aumentare la partecipazione
- Migliorare la sicurezza e trasparenza del processo elettivo
- Cambiare l'immagine e la percezione dell'Ente stesso
- Mantenere le prerogative dei Presidenti di Seggio

- Semplificare notevolmente le operazioni ed i tempi di allestimento
- Ottenere gli scrutini in tempi rapidi,
- Ottenere dati certi senza schede nulle o interpretabili.

Con l'adozione di un sistema di votazione online o elettronico in presenza la partecipazione potrà essere aumentata in maniera significativa considerando che potranno votare tutte le persone che hanno effettivamente diritto di voto ma sono impossibilitate a recarsi presso il seggio fisico per un'infinità di ragione diverse. Dalla residenza all'estero a motivi di lavoro. Rendere il processo di voto totalmente digitale permette di svolgerlo da qualsiasi parte del mondo con la sola necessità di avere accesso ad Internet e la documentazione necessaria.

La semplicità e chiarezza del processo di voto è di fondamentale importanza al fine di garantire elevati livelli di partecipazione

La trasparenza deriva da un processo di voto e di scrutinio automatizzato, fornito da una società terza indipendente e specializzata e team di professionisti con elevate competenze specialistiche. La gestione dei dati personali avviene nel pieno rispetto della normativa Privacy (GDPR).

1.2. Verifiche sulla piattaforma di voto ELIGO

La garanzia della segretezza del voto è stata verificata dall'Ente

GARANTE PRIVACY

Nel 2011, in occasione dello svolgimento di votazioni online di un'importante Cassa Previdenziale, è stato richiesto l'intervento del Garante della Privacy in merito alla verifica della segretezza del voto sulla piattaforma di e-voting fornita da IDTechnology srl. **Nella vigenza e in base al contenuto dell'allora D.Lgs. 196/2003,** così si è espresso il Garante per la protezione dei dati personali nel provvedimento conclusivo dell'istruttoria:

- *…"l'eventuale relazione tra elettori e preferenze di voto espresse non è registrata in alcuna tabella, nè è ricostruibile partendo dalle informazioni archiviate nei database*".
- *…"La comunicazione elettronica avviene tramite protocolli crittografici".*
- *..."Le misure descritte da ID Technology si valutano adeguate per impedire l'identificazione diretta e indiretta dei votanti e dei voti espressi, con la conseguenza che possono considerarsi insussistenti i paventati rischi di identificazione del votante*".

TRIBUNALE DI ROMA

Nel 2015, la Sentenza del Tribunale Ordinario di Roma con l'adozione della piattaforma ELIGO evoting:

"***Risultano approntate una serie di cautele tecnologiche idonee ad impedire un uso scorretto o improprio del voto e ad offrire le maggiori garanzie di riservatezza, segretezza e libertà di espressione del voto".***

Dopo il 31 marzo 2019, le Amministrazioni Pubbliche **acquisiscono esclusivamente servizi Infrastructure as a service (IaaS), Platform as a Service (PaaS) e SaaS qualificati dall'Agenzia per l'Italia digitale** e pubblicati sul Marketplace Cloud della PA.ELIGO è un servizio SaaS registrato sul portale AGID come fornitore qualificato. Utilizziamo anche un Cloud Provider registrato sul portale AGID.

AGID Agenzia per l'Italia digitale

https://cloud.italia.it/marketplace/service/750

1.3. Esperienze nel settore Università

La soluzione ELIGO sviluppata e specializzata per le esigenze universitarie è stata adottata negli ultimi anni dai seguenti Atenei pubblici e privati. Qui di seguito sono riportati **solo alcuni dei nostri clienti:**

Università degli studi di Roma "La Sapienza"	*Università degli Studi di Genova*
Università degli studi di Padova	*Università degli Studi di Ferrara*
Alma Mater Studiorum Università di Bologna	*Università degli Studi Suor Orsola Benincasa*
Humanitas University	*Università degli Studi "Magna Graecia" di Catanzaro*
Iuss - istituto universitario di studi superiori di Pavia	*Università degli Studi di Torino*
Università degli Studi di Verona	*Università degli studi di Trento*
Università degli Studi di Firenze	*Università degli studi della Campania Luigi Vanvitelli - Seconda Università degli studi di Napoli*
Università degli Studi di Foggia	*Università Cattolica del Sacro Cuore*
Politecnico di Torino	*Università degli studi di Brescia*

1.1. Esperienze nel settore Fondi e Casse

La soluzione ELIGO sviluppata e specializzata per le esigenze di Fondi e Casse previdenziali è stata adottata negli utlimi dai seguenti Enti. Qui di seguito sono riportati **solo alcuni dei nostri clienti:**

Fondo Pensioni del personale Gruppo BNL/BNP Paribas ITALIA	*CASAGIT – Cassa Autonoma di Assistenza Integrativa dei Giornalisti Italiani*
ENPAB – Ente Nazionale Previdenza Assistenza Biologi	*ENPACL – Ente Nazionale di Previdenza e Assistenza per i Consulenti del Lavoro*
ENPAM – Ente Nazionale di Previdenza ed Assistenza dei Medici per degli Odontoiatri	*ENPAPI – Ente Nazionale Previdenza Assistenza Professione Infermieristica*
EPPI – Ente di Previdenza dei Periti Industriali e dei Periti Industriali Laureati	*Fondaereo Fondo Pensione Complementare Naviganti del Trasporto Aereo*
Fondo Malattia Creberg - FIAM - FONDO INTEGRATIVO ASSISTENZA MALATTIA	*Fontex - Fondo di previdenza integrativa per i dipendenti della Texas Instruments Italia*
Fondo Pensione PREVIBANK	*INPGI Istituto Nazionale Previdenza Giornalisti Italiani "Giovanni Amendola"*

2. FUNZIONALITÀ GENERALI DEL SISTEMA DI VOTO

2.1. Organizzazione e processo di voto

2.1.1. Sintesi autenticazione e processo di voto

Breve sintesi del processi d'accesso front end nei confronti del votante

a. L'accesso al sistema ELIGO prevede l'autenticazione tramite vostro identity provider (di seguito SSO). Ogni votante potrà quindi accedere tramite il vostro portale con le proprie solite credenziali d'accesso. Il link d'accesso al sistema verrò inviato sull'email istituzionale dei singolo votante e verrà anche esposto all'interno dell'area riservata
b. Le comunicazioni tra votante e sistema di voto centrale vengono crittografate tramite connessione cifrata su protocollo https (certificato SSL/TLS) mediante certificato digitale a 256 bit.
c. Il vostro SSO comunica informazioni necessarie ad ELIGO per il controllo incrociato dell'anagrafica degli aventi diritto contenuta nel sistema per completare la prima fase del processo d'identificazione
d. Il processo d'identificazione è concluso ed il votante accede alla cabina elettorale virtuale
e. Il votante esprime le proprie preferenze di voto esclusivamente nelle schede di voto di propria competenza
f. Al momento del voto l'informazione voto / votante viene definitivamente persa e non potrà mai più essere ricostruita.

I dati relativi alle preferenze espresse (voti) sono mantenuti (opzionalmente in modalità crittografata) all'interno dell'apposito database, impedendone la leggibilità ed alterazione. Analogamente anche le password assegnate agli elettori sono mantenute in maniera protetta e crittografata nella relativa base dati.

Per la piena segretezza, in ELIGO non viene registrato alcun legame tra voto espresso e votante e le schede di voto, già anonime, vengono memorizzate in un database dedicato. Viene nativamente impedito dalla piattaforma il doppio voto. Viene garantito un elevato livello di sicurezza sui dati mediante l'utilizzo di due base dati distinte, dove i dati sensibili vengono mantenuti crittografati.

2.2. Monitoraggio e singole Commissioni Elettorali

2.2.1. Architettura generale

L'architettura della vostra votazione prevede una postazione centrale di controllo che può avere visione sull'andamento globale delle votazioni. Le votazioni saranno organizzate in un'unica area elettorale

2.2.2. Gestore dell'area centrale

Al termine delle votazioni il gestore dell'area elettorale trasmetterà copia degli scrutini al Decano. È applicata la crittografia della base elettorale con gestione delle chiave da parte del sistema di

Gli osservatori, eventualmente nominati, possono accedere alle aree elettorali di propria competenza e verificare lo stato di avanzamento di tutte le votazioni in essa presenti.

Figura 3 - Verifica avanzamento votazioni per utenti Osservatori

2.3. Accessibilità del servizio di voto

ELIGO è un sistema di voto elettronico esposto via web, accessibile da qualunque postazione internet dotata di un web browser e da qualsiasi device (smartphone, pc, tablet) senza necessità di installazione locale di altri software.

L'accesso al voto è regolato centralmente e quindi è possibile aprire e chiudere simultaneamente tutte le votazioni, senza riferimenti al tempo locale della postazione di voto.

Ogni elettore potrà accedere alla cabina di voto attraverso un apposito link inviato nella e-mail istituzionale e pubblicato sul portale di Ateneo

2.4. Adeguamento al Regolamento (UE 2016/679) GDPR

IDTechnology utilizza per il servizio ELIGO nelle sue varie versioni la soluzione Private Cloud di ARUBA con sede fisica dei dati e di eventuali back up ad Arezzo, Italia, Europa

I dati che sono collezionati dagli utenti sono quelli minimi richiesti per esercitare il diritto di voto comprendono i dati di connessione (IP sorgente, User Agent).

Non vengono installati cookies che facciano riferimento a servizi esterni alla piattaforma di voto ELIGO (per es: statistiche di accesso, collezione di informazioni attivita' utente) eccetto quello necessari per operazione di Single Sign On. In generale IDTechnology, dietro incarico, funge da Responsabile del trattamento dei dati identificativi di contatto e di connessione

Nella Policy Privacy saranno indicati:

- il titolare del trattamento
- la natura dei dati trattati
- le finalità del trattamento
- la base giuridica del trattamento
- le modalità del trattamento
- comunicazione e diffusione dei dati
- tempi di conservazione
- i diritti dell'utente e le modalita' per poterli esercitare

Minimizzazione dei dati (Art. 5 e 6 GDPR)

Nel rispetto dei citati articoli sul sistema ELIGO saranno presenti esclusivamente i dati necessari al processo di identificazione e di funzionamento della piattaforma. In merito ai dati identificativi dei votanti saranno presenti solo

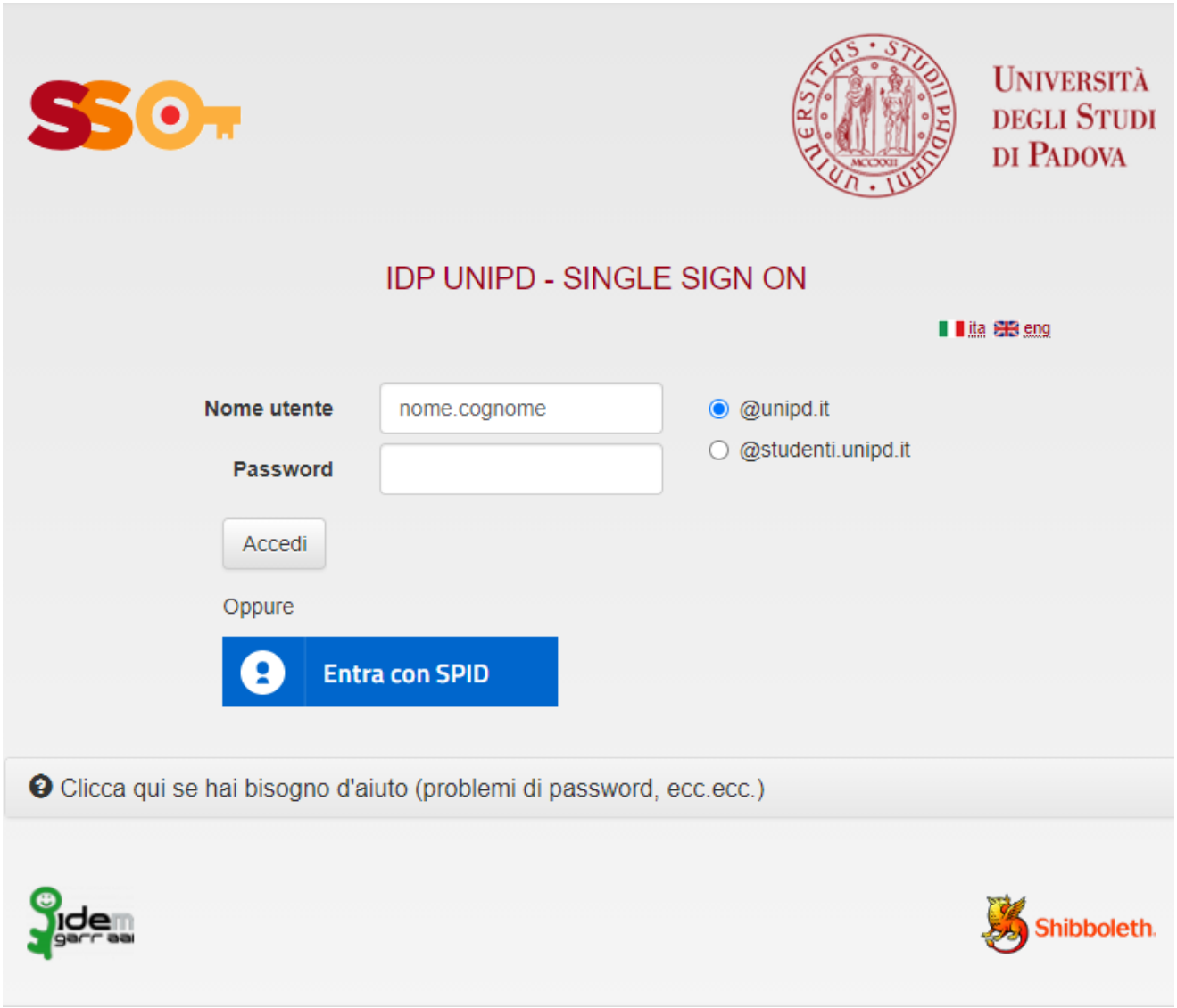
- Nome
- Cognome
- Codice univoco
- Email (solo se richiesto invio attestato via email)

ELIGO è stata ingegnerizzato sui principi di privacy by design e by default. Dalla banca dati, effettuando anonimizzazione e crittografia di tutte le informazioni inerenti dati privati degli utenti, ai canali interni ed esterni e alla verifica dell'aggiornamento degli ambienti applicativi ed obsolescenza delle macchine e servizi. Il tracking per la protezione avviene all'accesso dell'utente in cui viene verificata la versione del browser con una tabella di compatibilità. Eventuali browser che non supportano le librerie software

necessarie o che non implementano protocolli di cifrature delle sessioni vengono bloccati e viene invitato l'utente a utilizzare uno dei browser nelle versioni supportate

2.1. Prima fase d'identificazione

La prima fase d'identificazione è a carico del vostro SSO con le modalità ed interfaccia grafica prevista



2.2. Espressione delle preferenze

a. L'elettore verrà quindi indirizzato **esclusivamente alle schede di voto per cui ha diritto di voto**

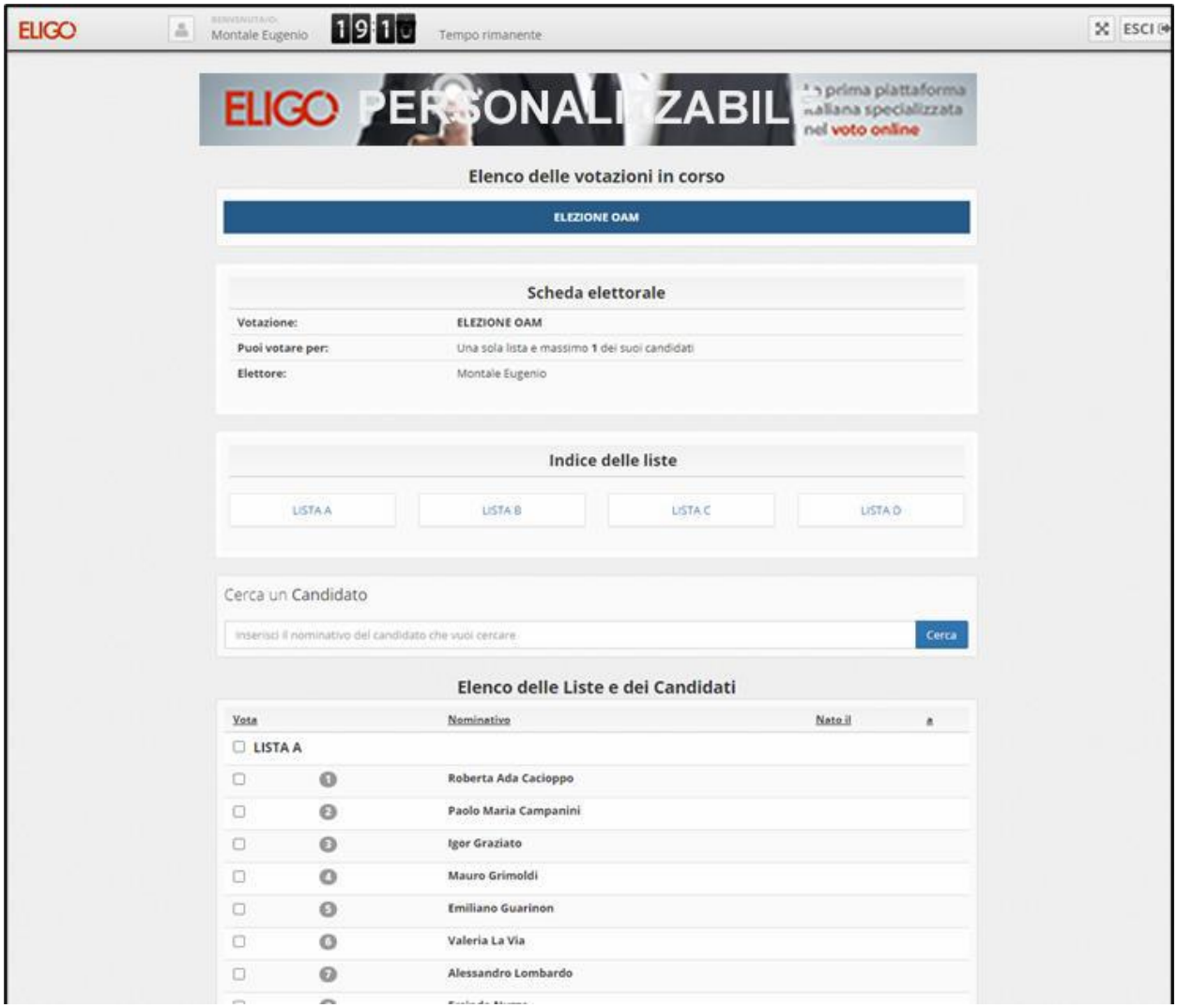


Figura 1 - Estratto di un esempio di scheda di voto su lista mostrata ai votanti

b. L'elettore assegnerà le preferenze, nel numero massimo stabilito, e confermerà la scelta. Ricordiamo che è sempre ammesso il voto di scheda bianca

Le preferenze espresse verranno riepilogate prima della conferma da parte del votante. All'atto di conferma delle preferenze, queste vengono memorizzate definitivamente nel sistema di voto.

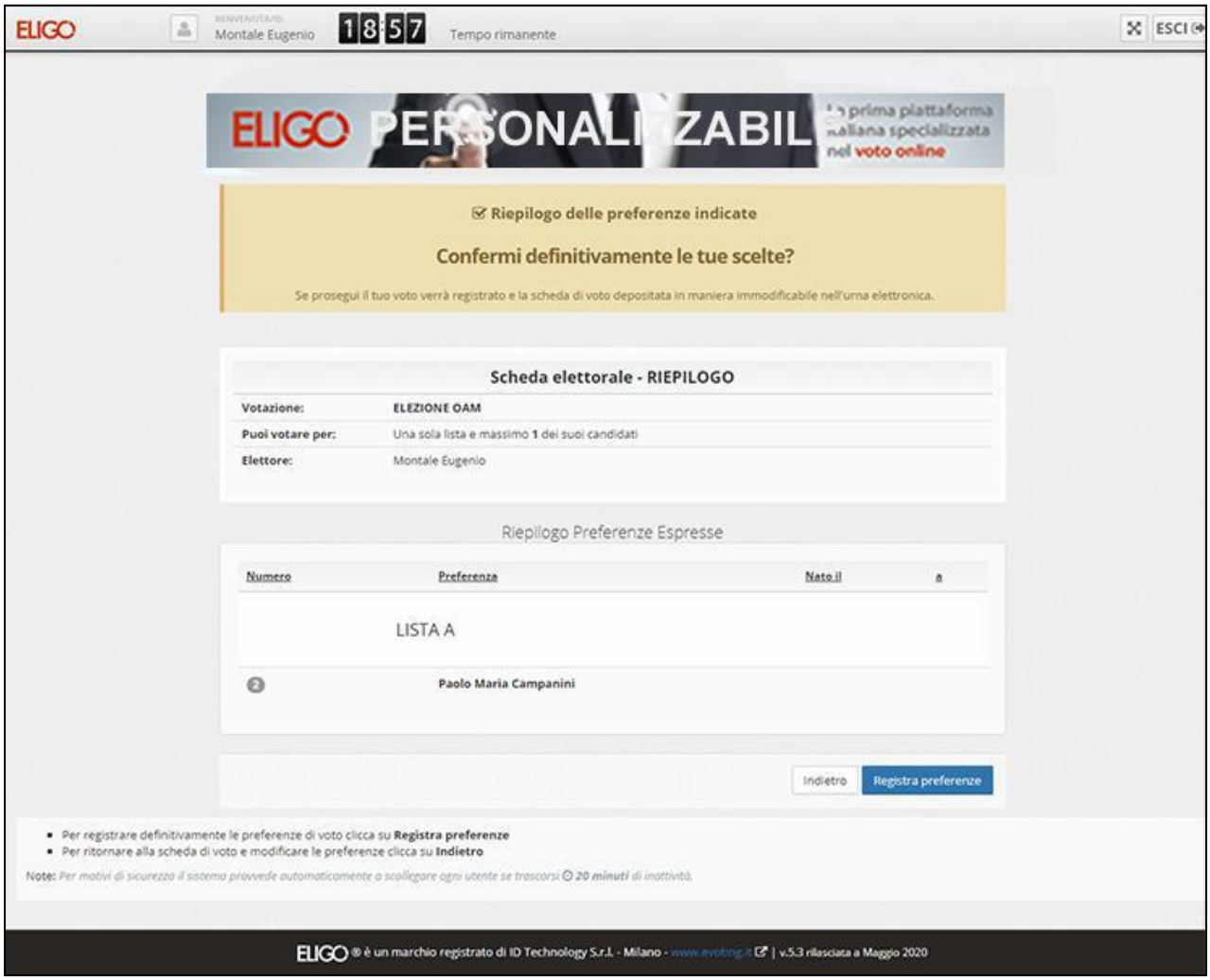


Figura 2 - Riepilogo preferenze espresse

Il sistema ELIGO fornisce al votante l'evidenza del voto espresso per ogni singola scheda prima di proseguire con la scheda successiva. ELIGO permette anche di consegnare un attestato di avvenuta votazione, assolutamente generico, via email oppure stampato. ELIGO può essere impostato per inviare l'attestato di avvenuta votazione in automatico all'indirizzo email associato al votante

2.3. Evidenza del voto espresso

La fase finale della registrazione di un voto nell'urna digitale Eligo, prevede che il sistema informi visivamente l'elettore della corretta esercitazione del voto.

L'elettore può provvedere alla stampa della pagina o richiedere la ricezione di una mail attestante l'avvenuta registrazione del proprio voto.

Figura 3 – Attestato di avvenuta votazione

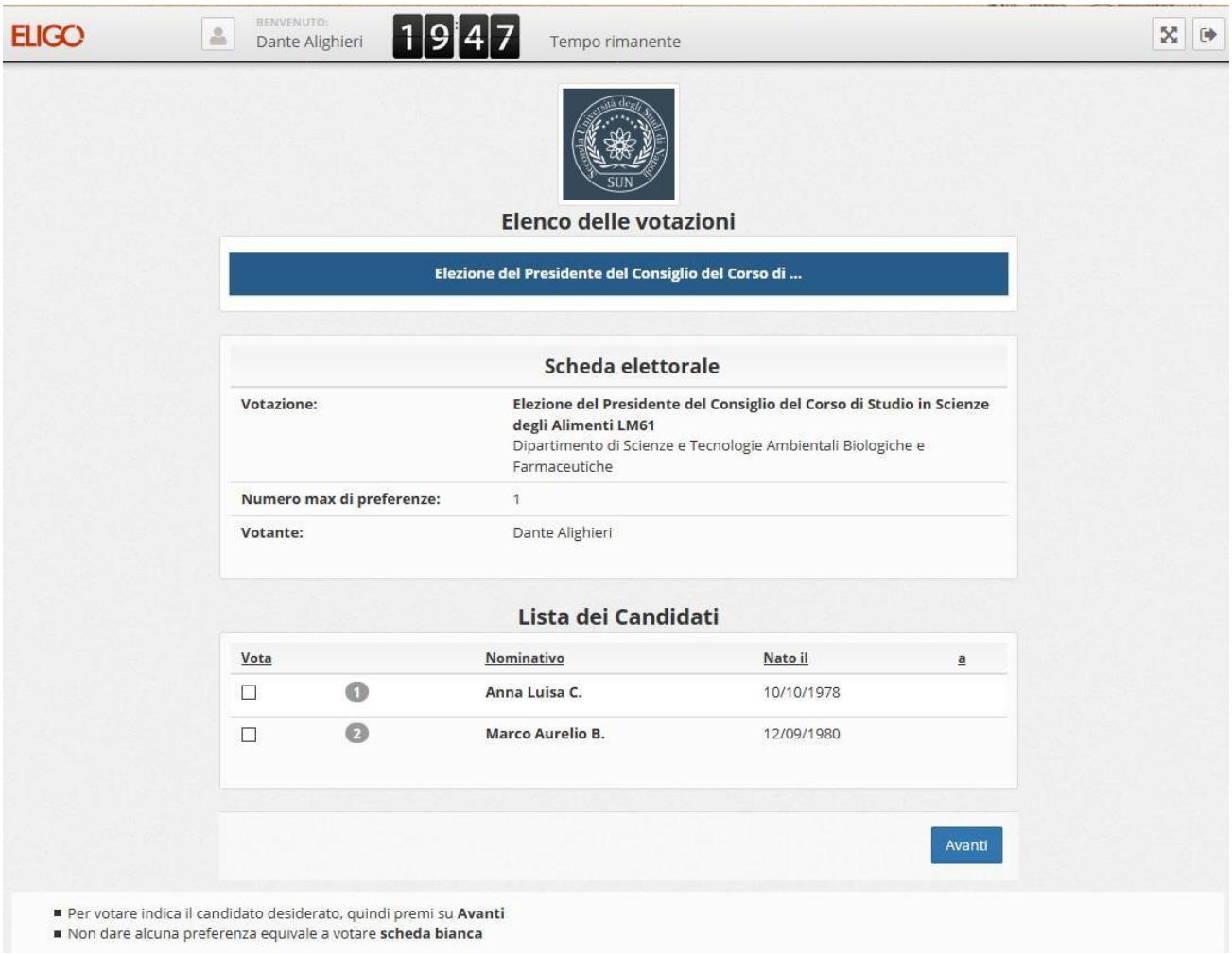


Figura 4 - Layout di una scheda di voto su Candidati

2.4. Gestione della Cifratura a doppia chiave

Eligo provvede a crittografare i voti registrati nell'urna digitale secondo l'algoritmo RSA.

La crittografia eseguita sui voti è del tipo “Asimmetrica”, tramite la quale i voti sono registrati e crittografati secondo una chiave pubblica e possono essere de crittografati esclusivamente tramite una opportuna chiave privata (si ricorda che un voto de crittografato non contiene comunque il legame voto/votante).

Durante la fase di approntamento delle aree di voto, viene attivata la crittografia dei voti con modalità a doppia chiave. Tramite apposita procedura interna il sistema ELIGO applicherà le chiavi di decrittografia.

A seguito dell’abilitazione della crittografia nell’area di voto, avviene la generazione delle chiavi crittografiche.

Viene qui sintetizzato il processo che prevede:

1. Generazione delle chiavi crittografiche

   Questa azione dà inizio al processo e provvede a generare le due chiavi di crittografia, pubblica e privata. Le chiavi vengono salvate in due distinti files nel sistema di voto e per maggiore sicurezza vengono codificati tramite l’applicazione di una crittografia simmetrica.

2. Salvataggio del file contenente la chiave privata

3. Verifica della validità della chiave privata

   È richiesta la sottomissione al sistema del file contenente la chiave privata scaricata per una ulteriore verifica finale. Se il sistema di voto verifica che la chiave non ha subito alterazioni, il processo di generazione si completa e viene completamente eliminato dal sistema di voto ogni riferimento alla chiave privata

4. Avvio scrutinio

   Il gestore dell’area avvio lo scrutinio dei voti

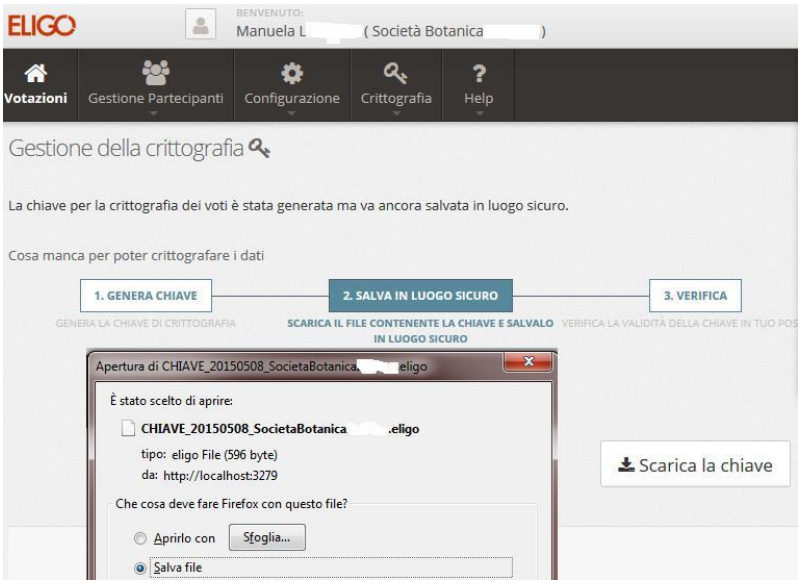


Figura 5 - Processo di consegna e verifica chiave privata

Il responsabile incaricato di mantenere la chiave privata conserverà la stessa (salvata in un opportuno file) fino alla chiusura delle votazioni, momento durante il quale tale chiave dovrà essere inviata al sistema di voto ELIGO per effettuare lo spoglio.

2.5. Chiusura delle votazioni ed avvio scrutinio e Report finali

Al termine dell'orario indicato verranno chiuse tutte le votazioni, impedendo qualsiasi accesso da parte dei votanti al sistema di voto. Prima dell'avvio dello scrutinio viene eventualmente verificato il raggiungimento del quorum necessario. Il dato d'affluenza sarà disponibile al gestore ed agli osservatori eventualmente nominati

A seguito della chiusura di ogni votazione, verrà generato lo **scrutinio dei voti** e consegnato al gestore dell'area elettorale in formato elettronico PDF non modificabile.

Per lo scrutinio, **ELIGO** genera un report standard per singola votazione, contenente le seguenti informazioni:

- dati della votazione (titolo, descrizione, data ed ora di apertura e chiusura)
- l'elenco ed il numero degli aventi diritto in anagrafe
- l'elenco nominale ed il numero dei votanti
- il numero di schede bianche
- l'elenco nominale dei candidati disposti in ordine decrescente di preferenze ricevute.

I voti conservati nella base dati relazionale dedicata (con modulo di crittografia attivato) sono sottoposti a crittografia e calcolo di impronta. In caso di qualsiasi alterazione di un voto registrato, il sistema impedirebbe le operazioni di scrutinio, informando della manomissione. I dati relativi ai voti registrati nella base dati saranno sempre conservati in forma crittografata. Durante la fase di spoglio i dati vengono decrittati esclusivamente in memoria mantenendo inalterata la base dati.

2.6. Infrastruttura

ID Technology si appoggia da diversi anni sui servizi cloud offerti da un service provider totalmente italiano, ARUBA S.p.a., dove rilasciamo e configuriamo l'infrastruttura utile a garantire il corretto funzionamento del sistema di voto ELIGO utilizzando il servizio Private Cloud offerto in modalità Iaas.

2.7. Certificazioni e Conformità dei provider di hosting / Cloud

In qualità di fornitore di servizi cloud, Aruba S.p.a. è dotata delle seguenti certificazioni:

- ISO 9001:2015,
- ISO 27001:2013,
- Cloud della PS / CSP qualificato,
- Dichiarazione di conformità ISO 27018:2014,
- Dichiarazione di conformità ISO 27017:2015,
- Dichiarazione di conformità ISO 27035:2016,
- ISO 14001:2015,
- ISO 50001:2011,
- Certificazione ANSI/TIA 942-B-2017,
- Certificazione ISAE 3402:2011 Type II Report,
- CISPE Service Declared - Servizi aderenti al Codice di Condotta CISPE per la protezione dei dati

Il Global Cloud Data Center di Aruba, dove verranno attivati i servizi offerti, è un data center localizzato ad Arezzo. Tutti gli impianti sono stati progettati e costruiti per soddisfare ed eccedere i massimi livelli di resilienza previsti dal livello Rating 4 (former Tier 4) di ANSI/TIA 942-B-2017.

Il Campus tecnologico è di 200.000 m² con 90.000 m² di superficie coperta destinata a data center dove vengono offerti massimi livelli di sicurezza logica e fisica e 7 diversi perimetri di controllo.

Sono disponibili fino a 90 MW di potenza, con produzione autonoma di energia idroelettrica e fotovoltaica, doppio power center multi-modulare con UPS a ridondanza 2N + 1, potenza personalizzabile fino a 40 kW per rack, generatori di emergenza ridondati con autonomia a pieno carico di 48 ore senza rifornimento, Data hall composta integralmente di muri tagliafuoco e tetto con doppia copertura isolante, Data Center carrier neutral con disponibilità di connettività gestita.

Il Private Cloud di Aruba Cloud è un servizio IaaS, che permette di creare Virtual Data Center contenenti server virtuali, firewall e reti, con possibilità di espansione o riduzione a seconda delle diverse esigenze del cliente. Il Private Cloud consente di possedere sia risorse computazionali, sia risorse di rete ad uso esclusivo.

Tutta l'infrastruttura è in alta affidabilità e resiliente ai guasti. L'intera struttura Private Cloud si appoggia su una solida componente di networking ridondata, interamente a 10 Gbit/sec. L'hardware impiegato per l'erogazione del servizio è dotato di ridondanza e lo storage è replicato.

Il servizio Private Cloud permette di acquistare quantità variabili di risorse computazionali (vCPU, RAM e HD), di rete (Virtual Lan, Firewall e IP pubblici) e servizi aggiuntiivi (Cloud DRaaS e Cloud Bare Metal Backup) da utilizzare tramite la console web VMware vCloud Director, per poter creare e gestire in completa autonomia data center Virtuali completi di funzionalità evolute come Firewall perimetrali, Bilanciatori e concentratori VPN.

Il servizio è pensato nell'ottica delle massime prestazioni: Rete interamente a 10 Gbit/sec, Server con processori ad elevatissima frequenza e di ultima generazione, Storage ridondato e replicato in modalità sincrona su di un data center secondario sono caratteristiche uniche che sono pensate per le aziende più esigenti.

Aruba eroga delle risorse computazionali che saranno poi utilizzate dal cliente secondo le proprie esigenze in maniera autonoma ed in totale sicurezza.

Questa soluzione ci consente di offrire ai clienti ELIGO prestazioni adattabili alla numerosità e contemporaneità degli elettori.

L'accesso alle macchine virtuali ospitanti i servizi di voto sarà consentito esclusivamente al personale ID Technology nominato ed autorizzato ad avvio progetto secondo i dettami GDPR, previa installazione e configurazione di apposita connessione VPN, necessaria ad impedire ogni tentativo esterno non autorizzato di accesso alle macchine.

Tutte le porte TCP/UDP in entrata/uscita sui servers saranno bloccate dal firewall hardware in dotazione (rimangono aperte esclusivamente le porte necessarie per la comunicazione web applicativa [http/https] e la porta necessaria all'inoltro e-mail).

L'intera infrastruttura cloud è protetta attraverso l'adozione di un firewall Fortigate VM-00, Software, Forticare e UTM di ultima generazione in grado di prevenire ed impedire attacchi malevoli ai sistemi.

Tale firewall garantisce funzionalità di web application firewall (WAF)

Le credenziali di accesso alla VPN, ai servers, all'interfaccia amministrativa del voto saranno a conoscenza esclusiva del personale tecnico specialista di prodotto, nominati dal referente tecnico ID Technology assegnato al processo.

Il Private Cloud di Aruba Cloud è un servizio IaaS, che permette di creare Virtual Data Center contenenti server virtuali, firewall e reti, con possibilità di espansione o riduzione a seconda delle diverse esigenze del cliente.

Il servizio Aruba Private Cloud è certificato AgID, così come il servizio di voto ELIGO, ed è disponibile anche per Pubbliche Amministrazioni e/o operatori che forniscono risorse alla Pubblica Amministrazione per l'erogazione dei propri servizi.

In quanto Cloud Service Provider qualificato di tipo C, infatti, Aruba offre soluzioni IaaS e Saas in linea con l'obbligo previsto dal 1° aprile 2019 secondo il quale le Pubbliche Amministrazioni possono utilizzare esclusivamente servizi Cloud erogati da Cloud Service Provider qualificati e presenti nel marketplace ufficiale dell'Agenzia per l'Italia Digitale.

Aruba è certificata ISO 27001 garantendo il rispetto di determinati standard di sicurezza nella gestione dei dati e delle informazioni aziendali, preservandone l'integrità, la riservatezza e la disponibilità.

2.8. Protezione tramite Firewall

Qualsiasi sia la configurazione scelta in termini di scalabilità, offriamo nativamente la protezione del server, o dei servers, tramite un **firewall Fortigate VM**.

Il sistema da noi adottato è FortiGate FW VM-00 con funzioni UTM, WAF ed abilitato a mitigare nativamente attacchi DDOS e minacce malevoli (intrusion prevention, SQL Injection)

Le caratteristiche e regole attivate sul firewall sono ad esempio:

Prevenzione delle intrusioni

La tecnologia IPS protegge automaticamente da minacce provenienti dalla rete. Oltre al rilevamento delle minacce basato sulla firma (signature-based threat detection), IPS esegue il rilevamento basato sulla verifica del traffico ed il controllo dei profili di comportamento di attacco.

Funzionalità abilitate

- Automatic Database Updates
- Protocol Anomaly Support
- IPS and DoS Prevention Sensor

Protezione dei contenuti
La tecnologia firewall Fortinet offre una protezione completa dei contenuti e della rete combinando l'ispezione stateful con una completa suite di funzionalità di sicurezza. Il controllo delle applicazioni, l'antivirus, IPS, filtri Web e VPN, costituiscono l'insieme delle funzionalità che identificano e mitigano le minacce di sicurezza.

Funzionalità abilitate

- NAT, PAT and Transparent (Bridge)
- Policy-Based NAT
- VLAN Tagging (802.1Q)
- Vulnerability Management

VPN
La tecnologia VPN di Fortinet fornisce comunicazioni sicure tra più reti e host, utilizzando le tecnologie SSL e IPsec VPN. Nel nostro caso la VPN è utilizzata per garantire al personale preposto la connessione RDP verso tutti i servers del cloud, rispettando la policy di chiusura totale delle porte in entrata sui nostri sistemi ad esclusione della porta 80 e 443.

Ispezione del traffico crittografato SSL

L'ispezione del traffico crittografato via SSL protegge i client endpoint ed i Web Server applicativi da minacce nascoste. L'ispezione SSL intercetta il traffico crittografato e lo ispeziona per le minacce prima di instradarlo alla sua destinazione finale

La componente RDMS è sempre protetta e non raggiungibile dalla rete pubblica.

2.9. Sicurezza fisica, logica ed applicativa

L'intera infrastruttura ospitante i nostri servizi e l'applicazione di voto ELIGO vengono periodicamente sottoposti a verifica attraverso la conduzione di Penetration Test e Vulnerability Assesments. Tali verifiche sono condotte da un operatore di mercato specializzato in sicurezza. L'ultima sessione di verifiche si è conclusa in data 15.10.2020

Quota parte delle verifiche condotte ci hanno permesso di accertare la piena conformità del sistema di voto nel rispetto e soddisfacimento delle linee guida OWASP TOP 10, qui di seguito riassunte.

Categoria Vulnerabilità	Esempi	Vulnerabilità Rilevata ?
A1 - Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the	NO

	interpreter into executing unintended commands or accessing data without proper authorization.	
A2 - Broken Authentication and Session Management	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.	NO
A3 - Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.	NO
A4 - XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.	NO
A5 - Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.	NO
A6 - Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.	NO
A7 - Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.	NO
A8 - Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.	NO

La sicurezza fisica (controllo accessi, continuità elettrica, antincendio) è garantita dal provider del servizio di cloud computing, che ha in carico anche la fornitura della banda di connessione e la sicurezza logica di accesso (firewall, antivirus perimetrali, log di connessione, monitoraggio).

Per quanto riguarda la sicurezza applicativa, **ELIGO** è stato progettato e realizzato da ID Technology in modo da aggiungere, alla sicurezza fisica e logica offerta dal contesto, ulteriori livelli di sicurezza applicativa, tra cui: la generazione casuale delle password di accesso, la classificazione degli utenti in profili predefiniti mappati sulle funzionalità dell'applicativo, la completa separazione del dato del voto dal dato del votante e l'opzione della **crittografia dei voti** a chiave doppia.

Le comunicazioni tra votante e sistema di voto centrale sono crittografate tramite connessione cifrata su protocollo https (SSL o SSL EV) mediante certificato digitale a 256 bit o superiore.

Ogni accesso al sistema di voto viene tracciato tramite l'abilitazione dei logs nativi del web server ospitante il servizio di voto ed ulteriormente tracciati in una opportuna tabella applicativa in cui viene registrata ogni operazione eseguita dai votanti; non vengono tracciate le scelte relative alle preferenze indicate nelle relative schede di voto.

Tracciabilità delle attività

Eligo prevede il tracciamento di tutte le attività eseguite sul sistema registrandole in una apposita tabella di log.

E' importante tenere conto che NON si tiene traccia, ad esempio nella fase di voto, delle preferenze indicate ma solo delle azioni svolte dal votante (Accesso, Apertura scheda di voto, Conferma dati, ecc.).

Nel cruscotto di Eligo è possibile verificare e scaricare quota parte dei dati di log, per avere evidenza delle date di apertura e chiusura delle votazioni, delle attività di gestione dell'anagrafe votanti e per verificare l'utenza che abbia eseguito tali azioni e quando.

2.10. Conservazione delle informazioni

Le informazioni saranno conservate dal Responsabile dei Dati secondo il Regolamento (GDPR) 2016/679, punto 29, 39, 45, e successivi. Successivamente alla restituzione dei dati al Titolare i dati personali vengono cancellati in maniera permanente , da tutti i nostri sistemi – inclusi i sistemi di back-up- entro 30gg salvo diverse pattuizioni formalizzate contrattualmente, adempimenti di legge o richieste dell'autorità giudiziarie