



DRESS

Sistema di e-voting per l'INFN

Michele Tota

michele.tota@Inf.infn.it



INFN-DRESS



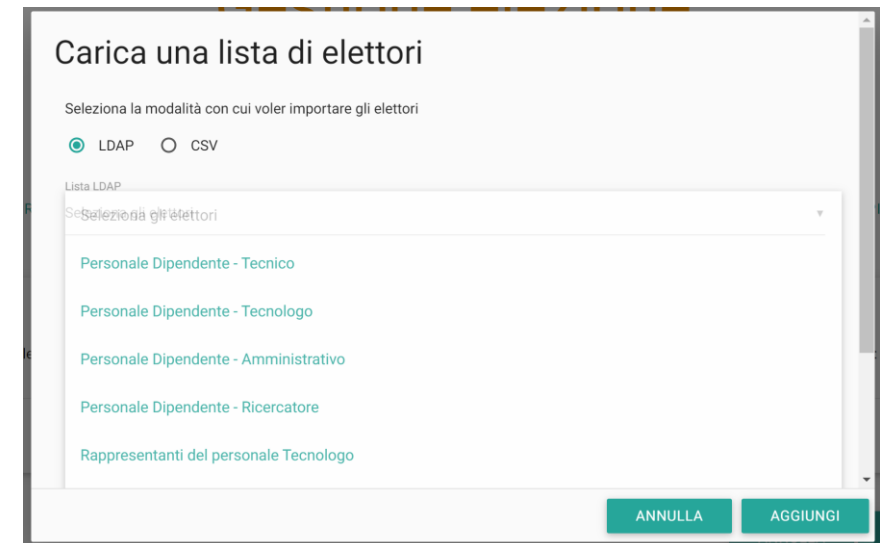
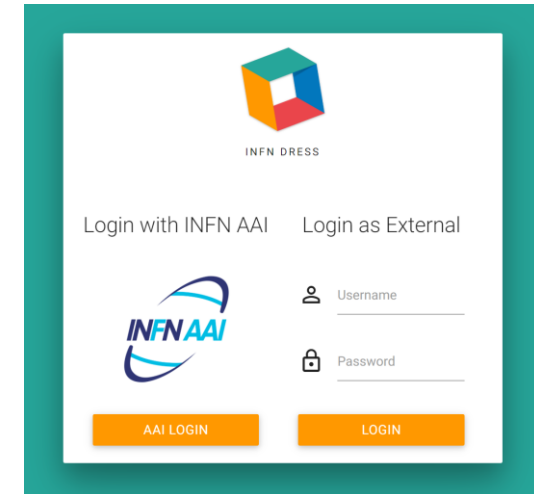
Può un sistema di e-voting fornire le stesse garanzie di un sistema di voto tradizionale ?

Quali caratteristiche deve avere un sistema di voto ?

- Democrazia
 - Solo elettori designati possono votare
 - Ogni elettore vota una volta sola
- Accuratezza
 - Il voto non può essere alterato
 - Un voto invalido non viene conteggiato
- Privacy
 - Impossibile risalire all'elettore
 - Impossibile mostrare il proprio voto

Democrazia

- DRESS utilizza per l'autenticazione
 - INFN-AAI
 - Autenticazione interna basata su username e password SOLO per utenti esterni
- Le autorizzazioni per votare recuperate da:
 - Attributi che qualificano un dipendente/ospite/associato registrato in GODiVA
 - Un elenco creato ad hoc in formato CSV



E' possibile inviare in modo sicuro un voto utilizzando un canale potenzialmente non sicuro (internet)?

Crittografia a chiave asimmetrica: RSA

RSA è basato sull'elevata complessità computazionale della fattorizzazione in numeri primi
Vengono scelti due numeri primi molto grandi p e q e viene calcolato

$$n = p \cdot q$$
$$\varphi(n) = (p - 1)(q - 1)$$

Si sceglie

e coprimo di $\varphi(n)$

d tale che $e \cdot d = 1 \pmod{\varphi(n)}$

(n, e) è la chiave privata

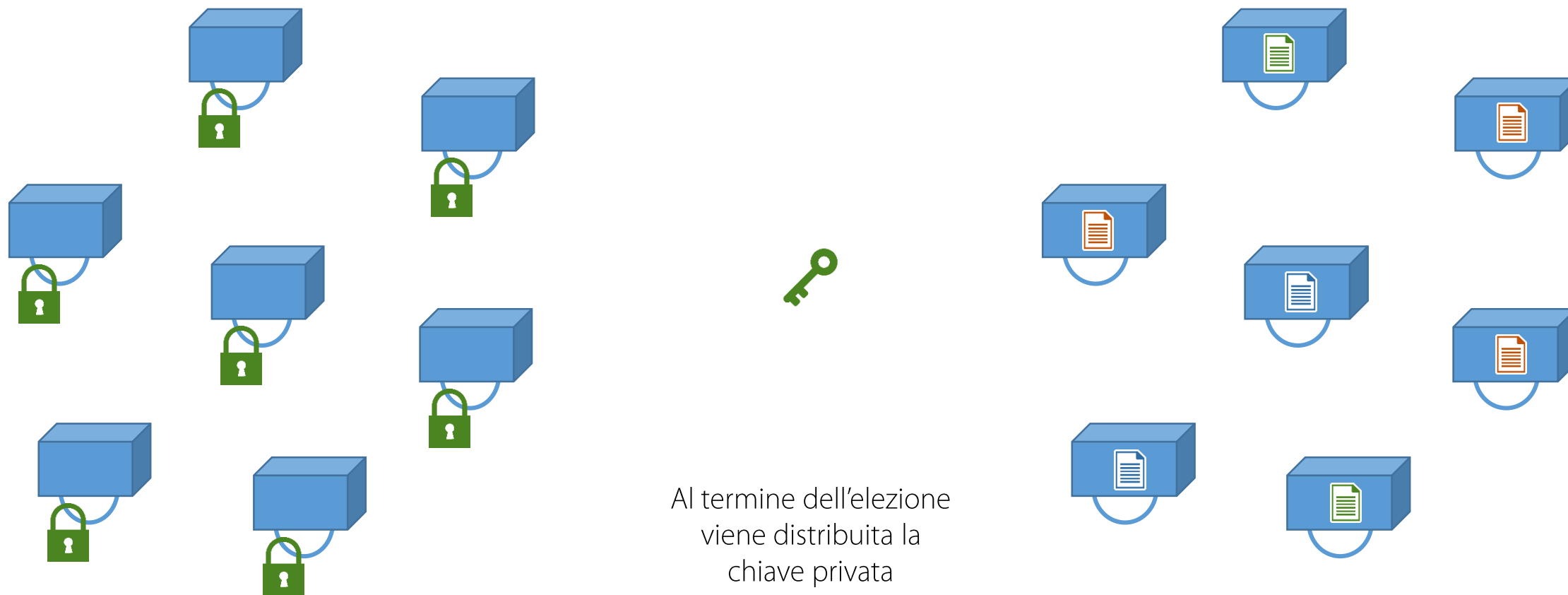
(n, d) è la chiave pubblica

Messaggio cifrato $M_c = M^e \pmod{n}$

Messaggio decifrato $M = M_c^d \pmod{n}$

[https://it.wikipedia.org/wiki/RSA_\(crittografia\)](https://it.wikipedia.org/wiki/RSA_(crittografia))

Raccolta voti cifrati



Come posso essere sicuro che il voto non venga replicato ?

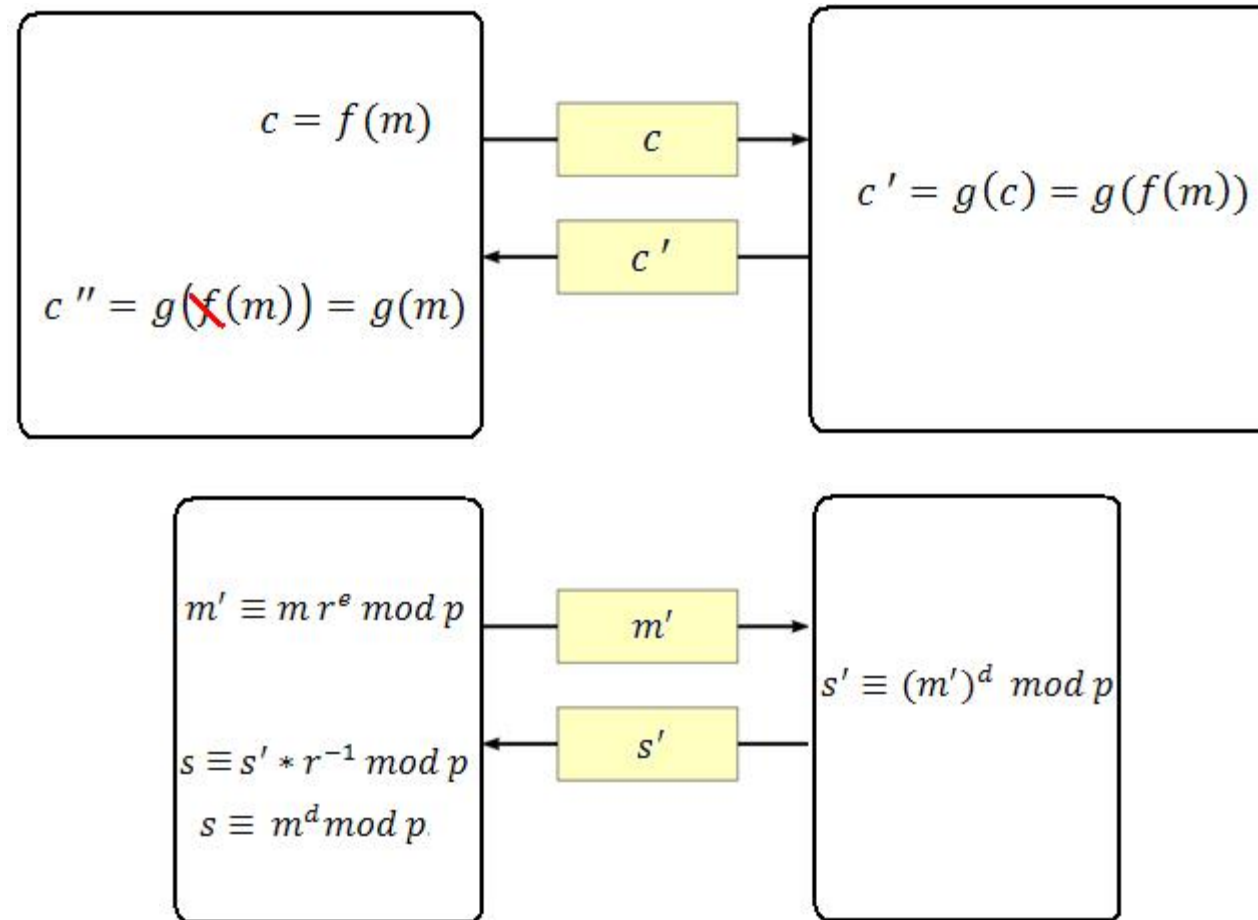
Richiesta di convalida del voto mantenendo la privacy

Il voto espresso deve essere convalidato da un'entità che può verificare il diritto di voto dell'elettore senza conoscere il voto espresso e riconoscere se l'elettore abbia già espresso il proprio voto.

- L'elettore inserisce il voto in una busta.
(Questa busta è particolare: è fatta di carta carbone)
- L'elettore sigilla la busta e la invia al convalidatore.
- Il convalidatore verifica che l'elettore abbia il diritto di voto, firma la busta e la rinvia al mittente.
- L'elettore aprendo la busta recupera il voto convalidato che verrà spedito con il metodo descritto in precedenza



RSA Blind signature



https://it.wikipedia.org/wiki/Blind_signature

Raccolta voti cifrati e validati



E se il convalidatore fosse corrotto o non raggiungibile ?

Come posso essere sicuro che il convalidatore non sia corrotto o non raggiungibile?

- Devo avere un numero di convalidatori N con $N \geq 3$
- Il numero di firme valide sul voto deve essere $> N/2 + 1$
- Durante lo spoglio elettorale vengono verificate le firme applicate su ogni voto e qualora il voto risultasse corrotto lo stesso viene considerato nullo.

Raccolta voti cifrati e validati da più convalidatori



Bene! Ma quando l'elezione è terminata esiste un modo per risalire a chi ha votato cosa ?



```
192.168.50.1:57077 [25/Jan/2019:21:10:30.575]  
fe_main- be main/sl 0/0/0/1/1 304 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:31.575]  
fe_main- be main/sl 0/0/0/1/1 304 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:32.575]  
fe_main- be main/sl 0/0/0/1/1 304 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:33.575]  
fe_main- be main/sl 0/0/0/1/1 304 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:34.575]  
fe_main- be main/sl 0/0/0/1/1 200 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:35.575]  
fe_main- be main/sl 0/0/0/1/1 200 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"
```

```
192.168.50.1:57077 [25/Jan/2019:21:10:31.575]  
fe_main- be main/sl 0/0/0/1/1 304 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:32.575]  
fe_main- be main/sl 0/0/0/1/1 304 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:33.575]  
fe_main- be main/sl 0/0/0/1/1 304 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:34.575]  
fe_main- be main/sl 0/0/0/1/1 200 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"  
  
192.168.50.1:57077 [25/Jan/2019:21:10:35.575]  
fe_main- be main/sl 0/0/0/1/1 200 180 -  
---- 1/1/0/I/O 0/0 "GET / HTTP/1.1"
```



Divide et impera

- Suddividere le operazioni su più server
- Distribuire i server su scala nazionale
- Disaccoppiare in modo tale che un amministratore di sistema con le informazioni in possesso non possa dedurre nessuna informazione in più di quelle che deve conoscere
- Per violare la privacy è necessario che gli amministratori si accordino tra di loro
- Attualmente l'installazione è solo ai LNF



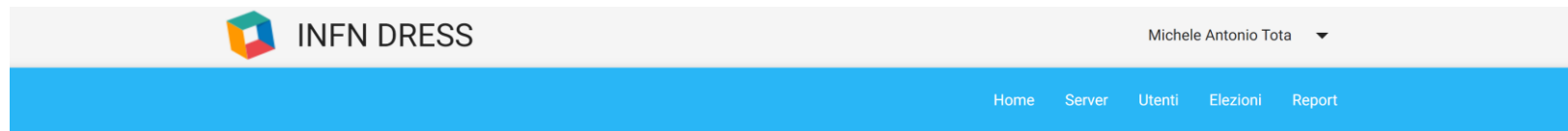
Come si crea un'elezione ?

Chi può creare un'elezione?

- Chiunque può creare elezioni.
- E' necessario avere il ruolo di amministratore
- Per richiedere il ruolo di amministratore (solo per la prima elezione):
 - Contattare il supporto dress@lists.Infn.it richiedendo la creazione di un'elezione
 - Verrà creata un'elezione «vuota» in cui il richiedente sarà nominato amministratore
 - L'elezione creata potrà essere modificata dal nuovo amministratore
- In futuro si controllerà un attributo su LDAP

Configurazione di un'elezione

- Amministrazione di DRESS: <https://dress.inf.infn.it/commissioner/>



Gestione elezioni

Elenco delle elezioni

	Ricerca elezione	Raggruppa per tipo	
✕	Test: Questa è una elezione di prova	18/10/2019 11:30:00	18/10/2019 15:00:00
✕	Formazione della rosa dei candidati alla carica di Direttore della sezione di Lecc...	09/09/2019 00:00:00	09/09/2019 18:00:00
✕	Sondaggio disciplinare concorsi - ricercatori	08/07/2019 10:00:00	22/07/2019 00:00:00
✕	Sondaggio disciplinare concorsi - tecnologi	08/07/2019 10:00:00	22/07/2019 00:00:00
✕	Elezione del rappresentante del personale ricercatore e tecnologo, dipendente o...	12/06/2019 08:00:00	18/06/2019 00:00:00
✕	Elezione del rappresentante del personale tecnico e amministrativo, dipendente ...	12/06/2019 08:00:00	18/06/2019 00:00:00

Configurazione di un'elezione

In questo step sono richieste le informazioni generali relative all'elezione:

- Descrizione (nome che comparirà nell'elenco delle elezioni)
- Data di inizio e fine
- Voto singolo o voto multiplo (verrà conteggiato solo l'ultimo)

Gestione elezione

Configura una nuova elezione

CONFIGURAZIONE DEFINIZIONE DEI SERVER DEFINIZIONE DEGLI UTENTI DEFINIZIONE DEI QUESITI RIEPILOGO

Descrizione
Elezione di prova

Data di inizio dell'elezione	Ora di inizio dell'elezione
30/10/2019	09:00
Data di fine dell'elezione	Ora di fine dell'elezione
30/10/2019	12:00

Abilita voto singolo (l'utente potrà votare soltanto una volta)

ANNULLA CONTINUA

Configurazione di un'elezione

E' possibile selezionare quali server coinvolgere per la gestione dell'elezione.

L'infrastruttura di DRESS avrà regole definite, questa schermata diventerà inutile!!!

CONFIGURAZIONE DEFINIZIONE DEI SERVER DEFINIZIONE DEGLI UTENTI DEFINIZIONE DEI QUESITI RIEPILOGO

<=>	Distributor
✓	Distributor
👤	Administrator
✓	Administrator
👤	Anonymizer
✓	Anonymizer
📄	Counter
✓	Counter


ANNULLA CONTINUA



Configurazione di un'elezione

Ogni elezione definisce tre tipologie di utenti:

- Elettorado attivo
- Amministratori
- Membri di commissione

CONFIGURAZIONE DEFINIZIONE DEI SERVER DEFINIZIONE DEGLI UTENTI DEFINIZIONE DEI QUESITI RIEPILOGO

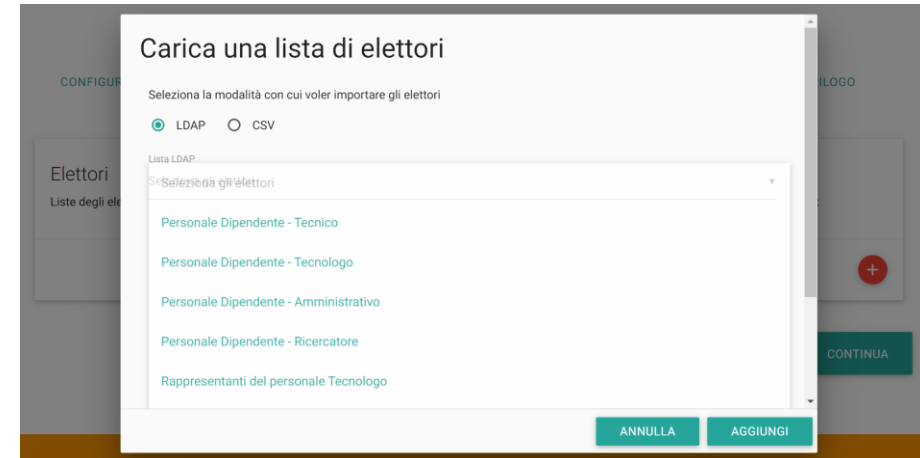
Elettori Liste degli elettori:	Amministratori Liste degli amministratori:	Commissione Lista dei membri di commissione:
		

Configurazione di un'elezione

E' possibile caricare la lista degli utenti in due modalità:

- LDAP (gruppi)
 - Contattare il supporto per richiedere l'inserimento di un gruppo mancante
- File CSV



Configurazione di un'elezione

- Formato del file CSV
 - 4 campi separati da virgola
 - 2 tipologie
 - INFN-AAI

INFN-AAI,017579c1-6567-4dbb-a2fc-6ef092c48d1e,Michele Tota,michele.tota@Inf.infn.it

INFN-AAI,452fa0d0-0774-477e-8893-f1d177f5b75e,Rossana Chiaratti,Rossana.Chiaratti@pd.infn.it

Tipo , **INFN uuid** , **Nome** , **Email**

- PBKDF2

PBKDF2,Mario Rossi,mario.rossi@example.com,xhyo3bq8

PBKDF2,Elisa Verdi,elisa.verdi@example.com,p7o1yl7x

Tipo , **Nome** , **Email** , **Password**

Configurazione di un'elezione

- Per ciascuna delle tre sezioni è possibile definire più gruppi di elettori anche di tipologia differente
- Facendo click sulla «x» viene eliminato l'intero gruppo dall'elezione



Configurazione di un'elezione


- Informazioni relative alla scheda elettorale
 - Titolo scheda
 - Istruzioni di voto
 - Definizione dei quesiti
 - Chiusa – singola
 - Chiusa – multipla
 - Aperta – singola
 - Aperta - multiple

CONFIGURAZIONE DEFINIZIONE DEI SERVER DEFINIZIONE DEGLI UTENTI DEFINIZIONE DEI QUESITI RIEPILOGO

Titolo della scheda elettorale
Elezione di prova

Istruzioni di compilazione
E' possibile esprimere un'unica preferenza.

Scheda elettorale



Configurazione di un'elezione

Quesito a risposta singola

Quesito


Quesito di test

Opzione 1

Risposta A

Opzione 2

Risposta B



Quesito a risposta multipla

Quesito

Quesito di test

Numero minimo di risposte

Numero massimo di risposte



Opzione 1

Testo

Opzione 2

Testo

Quesito a risposta singola aperta

Quesito

Testo del quesito

Quesito a risposta multipla aperta

Quesito

Testo del quesito

Numero opzioni massimo



Numero minimo di risposte

Numero massimo di risposte



Configurazione di un'elezione

- La scheda elettorale può essere costituita da più quesiti
- I quesiti non devono essere correlati
- Verrà mostrata l'anteprima dei quesiti così come saranno visibili sulla scheda elettorale

Scheda elettorale

Quesito di prova

- Risposta A
- Risposta B
- Risposta C

ELIMINA

Quesiti di prova a risposta aperta

Scrivi qui la tua preferenza

ELIMINA



ANNULLA

CONTINUA

Configurazione di un'elezione

- Riepilogo di tutte le informazioni inserite
- Cliccando «Salva» verrà creata l'elezione
- Riceverete un messaggio di successo oppure un messaggio di errore

Gestione elezione

Configura una nuova elezione

CONFIGURAZIONE DEFINIZIONE DEI SERVER DEFINIZIONE DEGLI UTENTI DEFINIZIONE DEI QUESITI **RIEPILOGO**

Configurazioni generali

Descrizione
Elezione di prova

Data di inizio dell'elezione	30/10/2019	Ora di inizio dell'elezione	09:00
Data di fine dell'elezione	30/10/2019	Ora di fine dell'elezione	12:00

Voto singolo
Abilitato

Server selezionati

Distributor	Administrator
Distributor	Administrator
Anonymizer	Counter
Anonymizer	Counter

Liste degli utenti

Lista dei votanti	Lista degli amministratori	Lista dei membri di commissione
Personale Dipendente - Tecnico gruppoStorage.csv	Tota	Enrico Maria Vincenzo Fasanelli

Scheda elettorale

Titolo della scheda elettorale
Elezione di prova

Istruzioni di compilazione
E' possibile esprimere un'unica preferenza.

Quesito di prova

Risposta A
 Risposta B
 Risposta C

Quesiti di prova a risposta aperta

Scrivi qui la tua preferenza

.....

Notifica ai votanti la creazione/modifica dell'elezione via mail

ANNULLA **SALVA**

Elezioni create

Gestione elezioni

Elenco delle elezioni

	<input type="text" value="Ricerca elezione"/>	Raggruppa per tipo <input type="checkbox"/>		
In programma	Test: questa è un'elezione non ancora iniziata	03/11/2019 09:00:00	03/11/2019 18:00:00	
In corso	Test: Questa è una elezione in corso	30/10/2019 11:30:00	30/10/2019 15:00:00	
Concluse	Test: questa è un'elezione conclusa	16/10/2019 00:00:00	17/10/2019 18:00:00	

Elezioni create

Gestione elezioni

Elenco delle elezioni

The screenshot shows a web interface for managing elections. At the top, there is a search bar labeled 'Ricerca elezione' and a toggle for 'Raggruppa per tipo'. Below this is a table of elections with three rows. The first row is marked 'In programma' (In program) with a yellow warning icon. The second row is marked 'In corso' (In progress) with a green checkmark icon. The third row is marked 'Concluse' (Completed) with a blue 'x' icon. To the right of each row are icons for editing (pencil), deleting (x), sending an email (envelope), and a menu (three dots). Orange arrows point from the labels 'In programma', 'In corso', and 'Concluse' to the status icons. Other orange arrows point from the labels 'modificare', 'eliminare', and 'mail agli elettori' to the respective action icons.

Status	Titolo	Start	End	Modificare	Eliminare	Mail agli elettori
In programma	Test: questa è un'elezione non ancora iniziata	03/11/2019 09:00:00	03/11/2019 18:00:00	[Pencil]	[X]	[Envelope]
In corso	Test: Questa è una elezione in corso	30/10/2019 11:30:00	30/10/2019 15:00:00	[Pencil]	[X]	[Envelope]
Concluse	Test: questa è un'elezione conclusa	16/10/2019 00:00:00	17/10/2019 18:00:00	[Pencil]	[X]	[Envelope]

ATTENZIONE: è possibile **modificare** ed **eliminare** un'elezione fino all'orario di inizio

Elezioni create

- Cliccando sul nome dell'elezione si vedrà il riepilogo
- Per le elezioni in corso (se è stato abilitato il voto singolo) verrà mostrato il dato relativo all'affluenza
- Per le elezioni concluse (se è stato abilitato il voto singolo) verrà mostrato il dato relativo all'affluenza e l'elenco degli elettori che hanno espresso il voto
- Nella sezione «Liste degli utenti» è possibile effettuare il download delle varie liste in formato PDF

Affluenza al 05/06/2019: **41.228 %**

(47 elettori su 114)

[Lista degli elettori che hanno espresso il proprio voto](#)

Liste degli utenti

File contenente la lista dei votanti

[Lista dei votanti in PDF](#)

File contenente la lista degli amministratori

[Lista degli amministratori in PDF](#)

File contenente la lista dei membri di commissione

[Lista dei membri di commissione in PDF](#)




Come visualizzare i risultati di un'elezione conclusa ?

Risultati dell'elezione

- In Report sono elencate tutte le elezioni concluse per le quali l'utente autenticato è
 - Amministratore
 - Membro di commissione

Gestione report elezioni

Elenco delle elezioni concluse

 Test: Questa è una elezione di prova	18/10/2019 11:30:00	18/10/2019 15:00:00
 Concorso fotografico WS CCR 2019	04/06/2019 15:30:00	05/06/2019 19:00:00
 votazione poster workshop CCR 2019	04/06/2019 15:30:00	05/06/2019 19:00:00

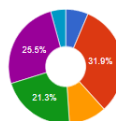
Risultati dell'elezione

Votazione poster workshop CCR 2019

I poster sono esposti vicino all'area sponsor, di fronte alla Sala Maria Luisa. E' possibile esprimere un'unica preferenza.

permalink: <https://dress.lnf.infn.it/commissioner/report?id=H8KW3AJDvXvBygb5RJO2KdQPwz1qbp>

Quale poster ritieni più interessante ed innovativo?



- "CLOUD di scoglio quando il computing incontra i Livornesi" (Autori: S. Arezzini, A. Ciampa, E. Mazzoni)
- "The ISOLPHARM_Ag - Simulazioni Monte Carlo con kubernetes" (Autori: L. Zangrando, M. Sgravato, M. Veriato, A. Andrighetto, M. Ballan)
- "Insight RIADA" (Autore: D. Castrì)
- "Il sistema di monitor on-line dell'esperimento PADME alla BTF di Frascati" (Autori: F. Ferrarotto, E. Leonardi, A. Ruggiero, F. Safai Tehrani, E. Vilucchi)
- "AMICO Apparato Milanese per il Calcolo Opportunistico" (Autori: F. Leveraro, F. Milanini, L. Perini, F. Preiz, D. Rebato, P. Salvestrini, M. Villapiana)
- Schede bianche

Preferenze	Voti	%
"The ISOLPHARM_Ag - Simulazioni Monte Carlo con kubernetes" (Autori: L. Zangrando, M. Sgravato, M. Veriato, A. Andrighetto, M. Ballan)	15	31.91 %
"AMICO Apparato Milanese per il Calcolo Opportunistico" (Autori: F. Leveraro, F. Milanini, L. Perini, F. Preiz, D. Rebato, P. Salvestrini, M. Villapiana)	12	25.53 %
"Il sistema di monitor on-line dell'esperimento PADME alla BTF di Frascati" (Autori: F. Ferrarotto, E. Leonardi, A. Ruggiero, F. Safai Tehrani, E. Vilucchi)	10	21.28 %
"Insight RIADA" (Autore: D. Castrì)	5	10.64 %
"CLOUD di scoglio quando il computing incontra i Livornesi" (Autori: S. Arezzini, A. Ciampa, E. Mazzoni)	3	6.38 %
Schede bianche	2	4.26 %

Riepilogo dati elettorali

Riepilogo	
Voti ricevuti	47
Aventi diritto di voto	114
Affluenza	41.23 %
Lista degli elettori che hanno espresso il proprio voto	

Permalink per distribuire i risultati dell'elezione (non richiede autenticazione)

Riepilogo dei dati elettorali

- Voti ricevuti
- Aventi diritto di voto
- Affluenza
- Lista degli elettori che hanno espresso il voto

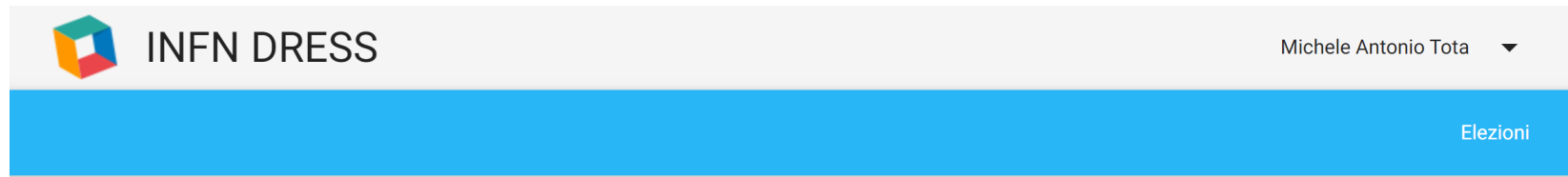
Pulsante per effettuare il download dei risultati in formato PDF o XLS

Per ogni quesito elettorale viene mostrato, per ogni opzione, il numero di voti ricevuti e la percentuale dei voti ricevuti sul totale dei voti ricevuti.

Come si vota ?


Come si vota ?

- Elezioni attive su DRESS: <https://dress.inf.infn.it/>



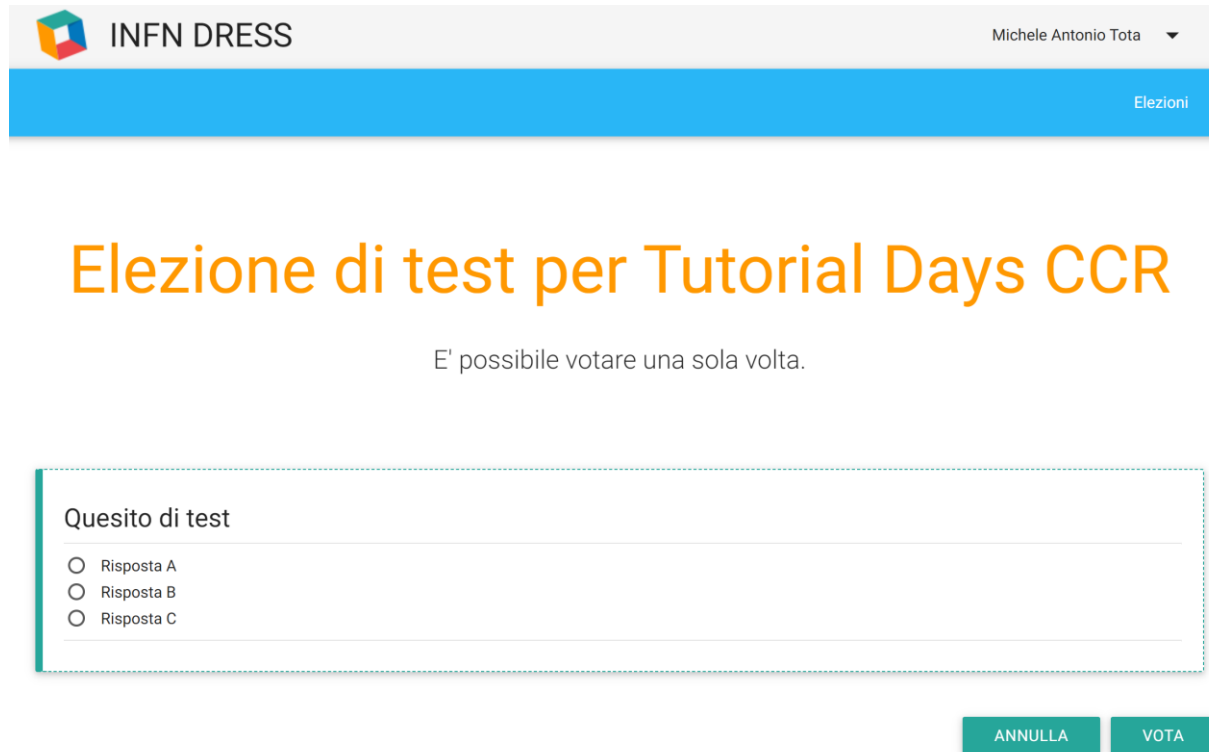
Elezioni

Elenco delle elezioni disponibili

 Elezione di test per Tutorial Days CCR	23/10/2019 15:25:00	23/10/2019 15:35:00
--	---------------------	---------------------

Come si vota ?

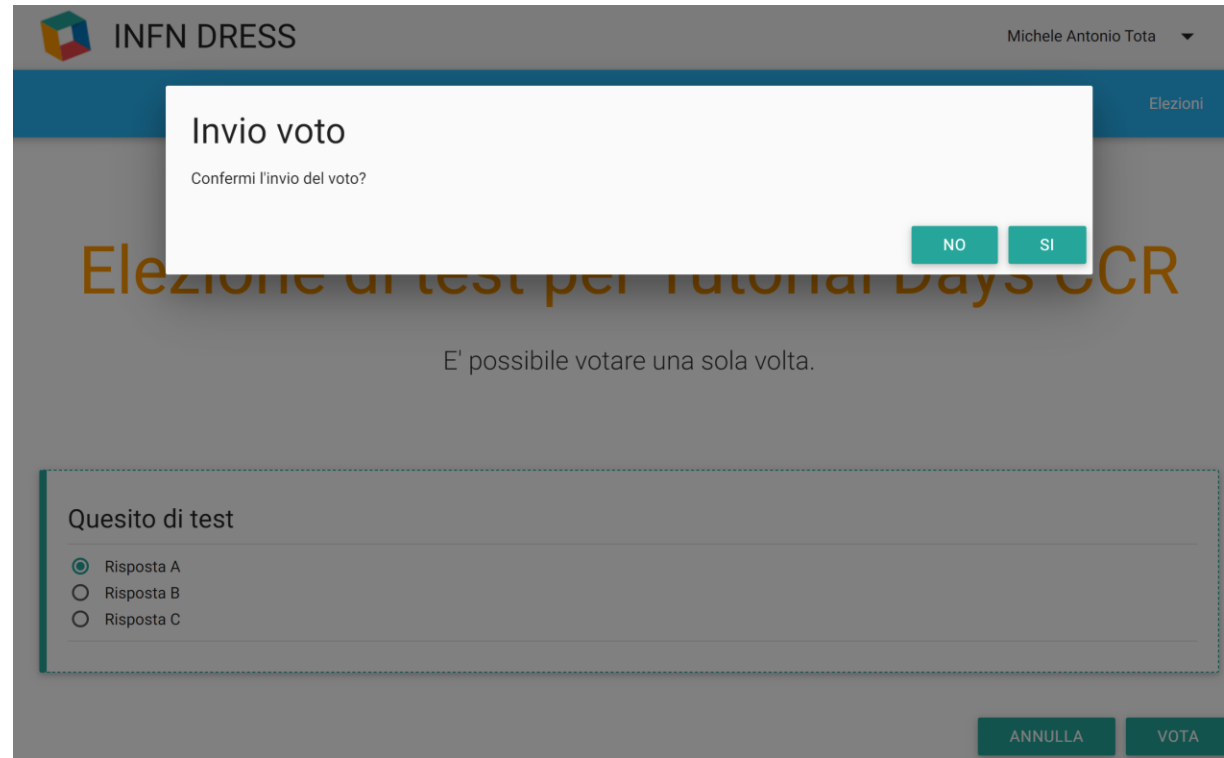
- Selezionando l'elezione di interesse viene aperta la scheda elettorale



The screenshot shows the INFN DRESS voting interface. At the top, there is a header with the INFN DRESS logo and the name 'Michele Antonio Tota' with a dropdown arrow. Below the header is a blue navigation bar with the word 'Elezioni'. The main content area features the title 'Elezione di test per Tutorial Days CCR' in orange, followed by the instruction 'E' possibile votare una sola volta.' Below this is a dashed box containing a 'Quesito di test' section with three radio button options: 'Risposta A', 'Risposta B', and 'Risposta C'. At the bottom right, there are two buttons: 'ANNULLA' and 'VOTA'.

Come si vota ?

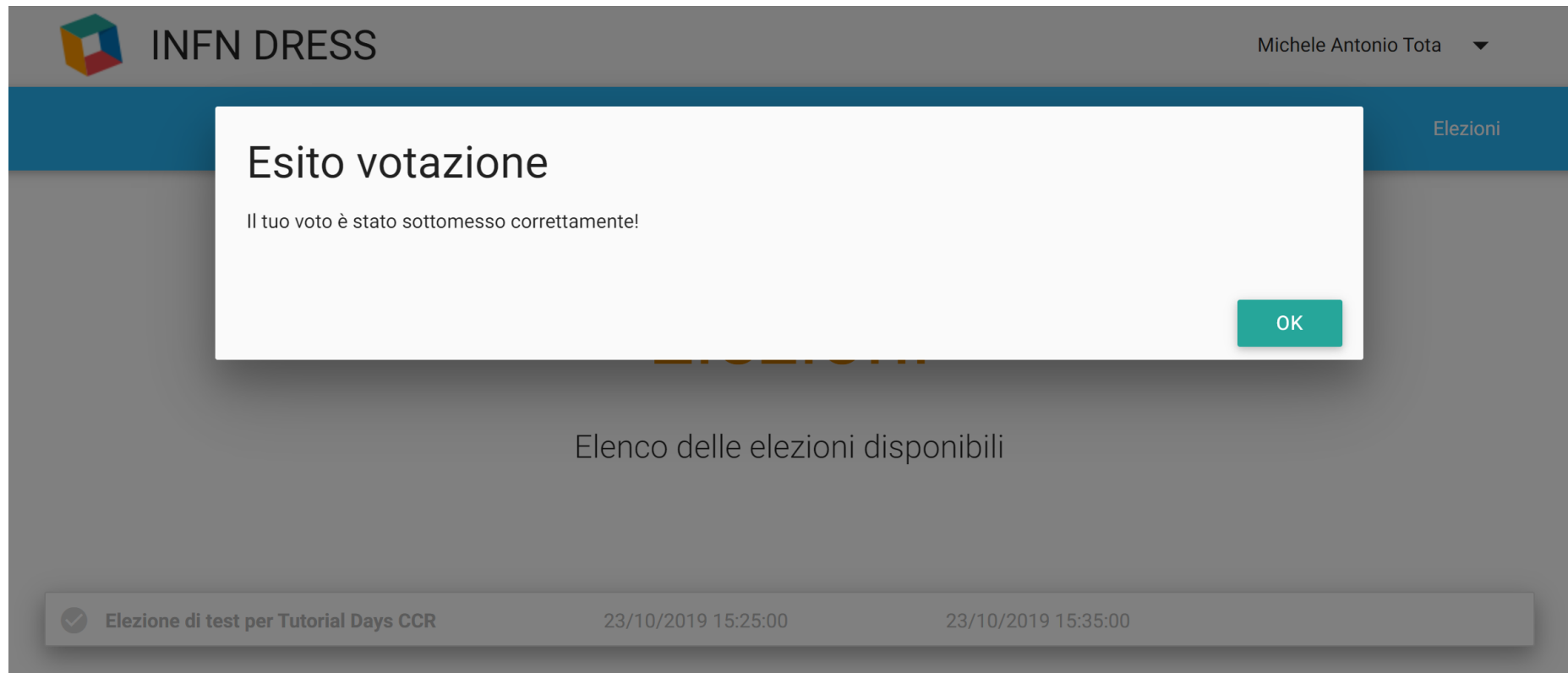
- Viene richiesta la conferma dell'invio del voto per evitare invii involontari



The screenshot displays the INFN DRESS web application interface. At the top left is the INFN DRESS logo, and at the top right is the user name "Michele Antonio Tota" with a dropdown arrow. A blue navigation bar contains the word "Elezioni". A white modal dialog box is centered on the screen with the title "Invio voto" and the text "Confermi l'invio del voto?". Below the text are two teal buttons labeled "NO" and "SI". The background is dimmed and shows the heading "Elezione di test per Tutorial Days CCR" and the text "E' possibile votare una sola volta.". Below this, there is a section titled "Quesito di test" with three radio button options: "Risposta A" (selected), "Risposta B", and "Risposta C". At the bottom right of the page are two teal buttons labeled "ANNULLA" and "VOTA".

Come si vota ?

- L'utente viene informato che il voto è stato sottomesso correttamente

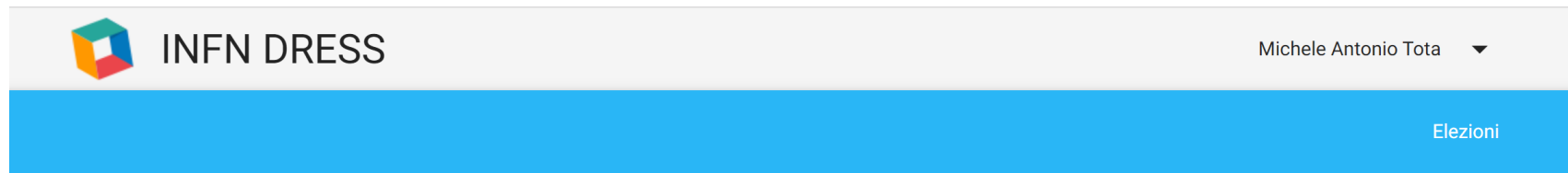


The screenshot displays the INFN DRESS web application. At the top left is the logo and name 'INFN DRESS'. At the top right, the user's name 'Michele Antonio Tota' is shown with a dropdown arrow. A blue navigation bar contains the word 'Elezioni'. A white modal dialog box is centered on the screen with the title 'Esito votazione' and the message 'Il tuo voto è stato sottomesso correttamente!'. A green 'OK' button is located in the bottom right corner of the modal. Below the modal, the text 'Elenco delle elezioni disponibili' is visible. At the bottom of the page, a table lists available elections.

✓ Elezione di test per Tutorial Days CCR	23/10/2019 15:25:00	23/10/2019 15:35:00
--	---------------------	---------------------

Come si vota ?

- Se l'elezione ammette voto singolo, l'elezione attiva per cui si è già votato non è più selezionabile.



INFN DRESS

Michele Antonio Tota ▼

Elezioni

Elezioni

Elenco delle elezioni disponibili

<input checked="" type="checkbox"/> Elezione di test per Tutorial Days CCR	23/10/2019 15:25:00	23/10/2019 15:35:00
--	---------------------	---------------------

Sviluppo software di DRESS

- Il software è stato sviluppato ai LNF
 - Ramon Orru' (non più dipendente INFN)
 - Michele Tota
- Autenticazione con minimo privilegio Paranoid Authentication
 - Dael Maselli



INFN-DRESS

Grazie per l'attenzione !!!

Domande ?

Michele Tota

michele.tota@Inf.infn.it

