



Berner Fachhochschule  
Haute école spécialisée bernoise  
Bern University of Applied Sciences

# Universelle Verifizierbarkeit des Genfer E-Voting Systems

# Inhalt

- ▶ Anforderungen
- ▶ Meilensteine
- ▶ Projektplan
- ▶ Mockup Prototyp
- ▶ Klassendiagramm
- ▶ Live Demo

# Anforderungen

## 2.1.1 Allgemeine Anforderungen

ID	Beschreibung	Priorität	Status
A.1	Alle Tests von der Projektarbeit 2 sind nach Definition implementiert.	Muss	Geprüft
A.2	Die bestehend Applikation zu Visualisierung des Genfer E-Voting System wird mit dem Verifier vervollständigt	Muss	Geprüft
A.3	Eine Konsolenanwendung um die Tests lokal auszuführen wird entwickelt. Dazu ist eine Schnittstelle zur Bestehenden Applikation nötig.	Kann	Geprüft
A.4	Die Applikation kann in Deutsch, Englisch und Französisch genutzt werden	Kann	Geprüft
A.5	Ein Script für die Generierung der Abstimmungsdaten einer Volksabstimmung wird entwickelt.	Kann	Geprüft

## 2.1.2 Verifier Visualisierung

ID	Beschreibung	Priorität	Status
A.6	Der Benutzer muss jederzeit nachvollziehen können, wie viel der Verifier schon getestet hat und bei welchem Test er gerade ist.	Muss	Geprüft
A.7	Der Benutzer erhält am Ende der Tests einen Überblick, welche Tests erfolgreich waren und welche nicht.	Muss	Geprüft
A.8	Im Überblick gibt es die Möglichkeit zu jedem Test detaillierte Informationen anzuzeigen	Muss	Geprüft
A.9	Der Benutzer kann das Ergebnis als PDF exportieren	Kann	Geprüft

# Meilensteine

- ▶ M1: Projekt Initialisierung ist fertig / Es können nun Anpassungen an der Bestehenden Applikation gemacht werden.
- ▶ M2: Implementation des Backends ist Abgeschlossen
- ▶ M3: Die GUI-Programmierung ist Abgeschlossen
- ▶ M4: Das Backend ist mit dem Frontend verknüpft, Alle Muss-Kriterien sind erfüllt
- ▶ M5: Alle Kann-Kriterien wurden erfüllt.
- ▶ M6: Dokumentation ist abgeschlossen

# Projektplan

Projekt Aufgaben			38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
							M1			M2			M3		M4		M5		M6
<b>Konzept und Planung</b>																			
Anforderungen und Meilensteine definieren	soll																		
	ist																		
Architektur und Prototyp(Mockup)	soll																		
	ist																		
<b>M1: Projekt Initialisieren</b>																			
Bestehende Applikation editieren können	soll																		
	ist																		
<b>M2: Implementation Python</b>																			
Von jeder Kategorie mindestens ein Test Implementieren	soll																		
	ist																		
Softwaresesing umsetzen	soll																		
	ist																		
<b>M3: GUI-Programmierung</b>																			
GUI Programmierung nach Prototyp	soll																		
	ist																		
<b>M4: Verknüpfung Backend/Frontend</b>																			
Alle Teste in Python implementieren	soll																		
	ist																		
Backend und Frontend verknüpfen / Alle Muss-Kriterien erfüllen	soll																		
	ist																		
<b>M5: Applikation erweitern</b>																			
Kann-Kriterien erfüllen	soll																		
	ist																		
<b>M6: Dokumentation</b>																			
Poster, Finaltag, Präsentation,Film	soll																		
	ist																		
Dokumentation ergänzen	soll																		
	ist																		



Berner Fachhochschule  
Haute école spécialisée bernoise  
Bern University of Applied Sciences

# Mockup Prototyp



Overview



Election Admin



Printing Authority



Voter



Election Authorities



Bulletin Board



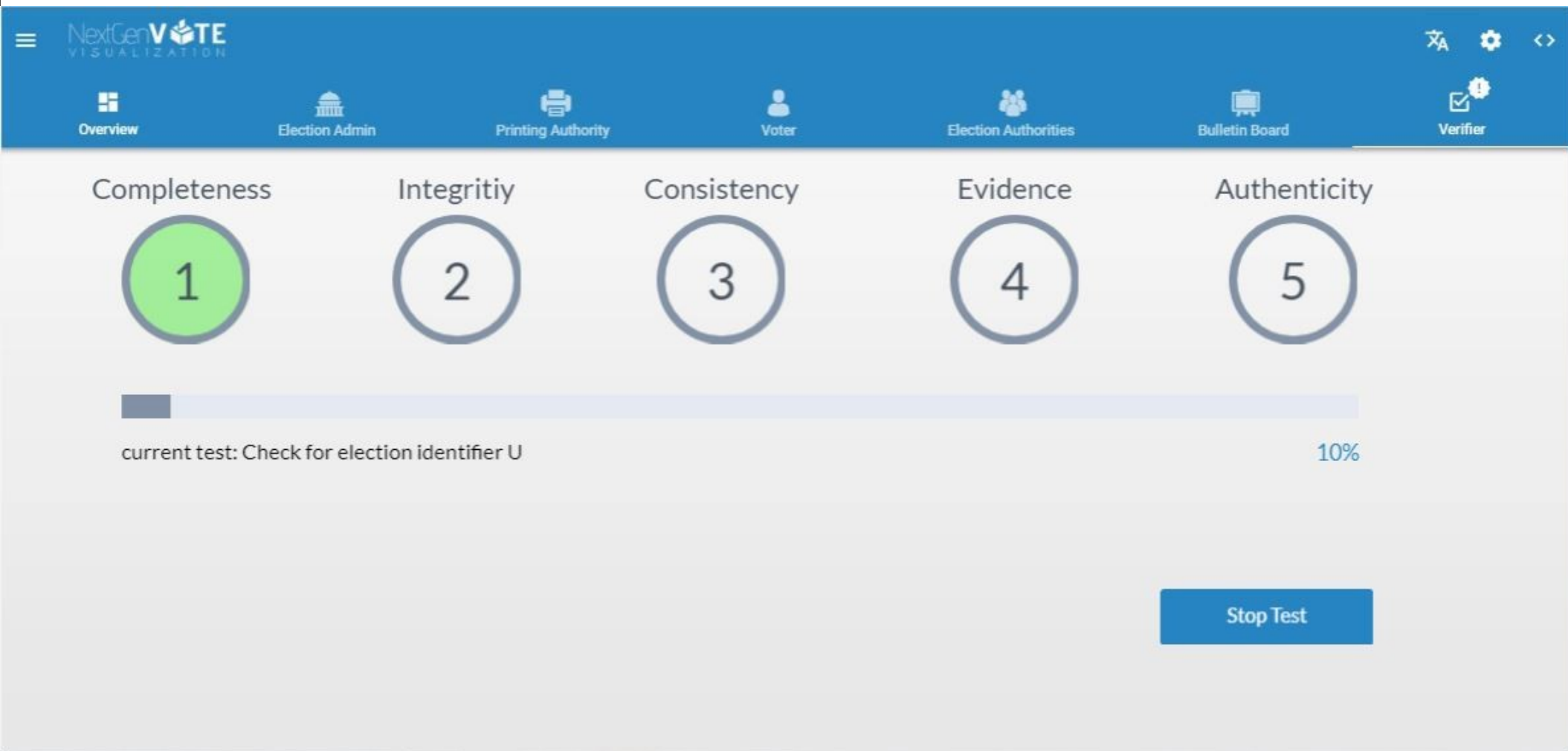
Verifier

## Verifier

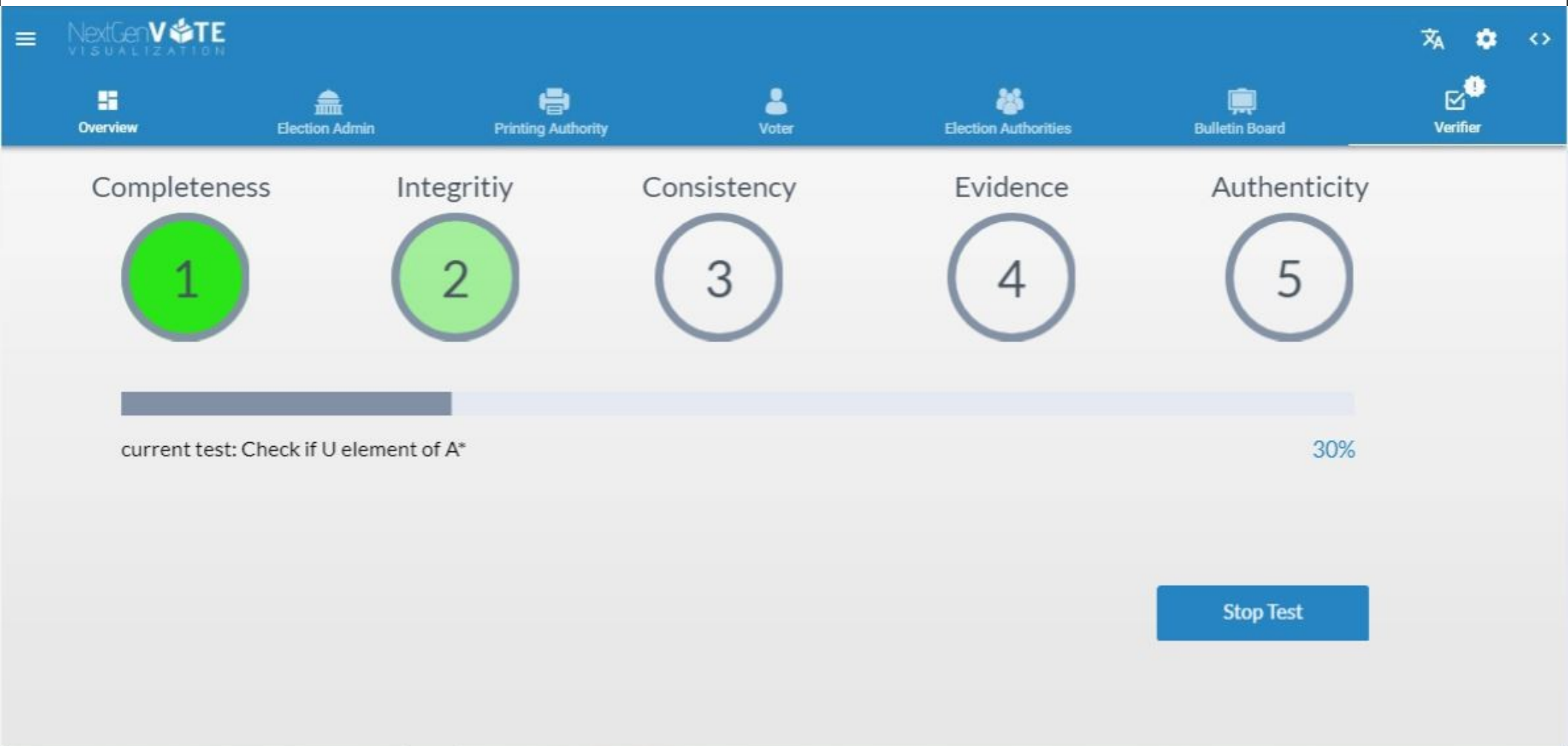
The universal verifiability is the requirement of the Swiss Government to apply an e-voting System. This Bachelor-Thesis shows, how a Verifier could look like and how it would work.



START TESTS







Completeness



Integrity



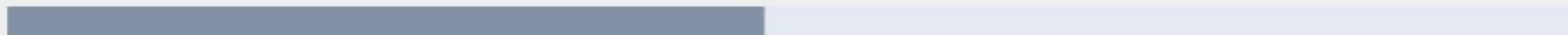
Consistency



Evidence



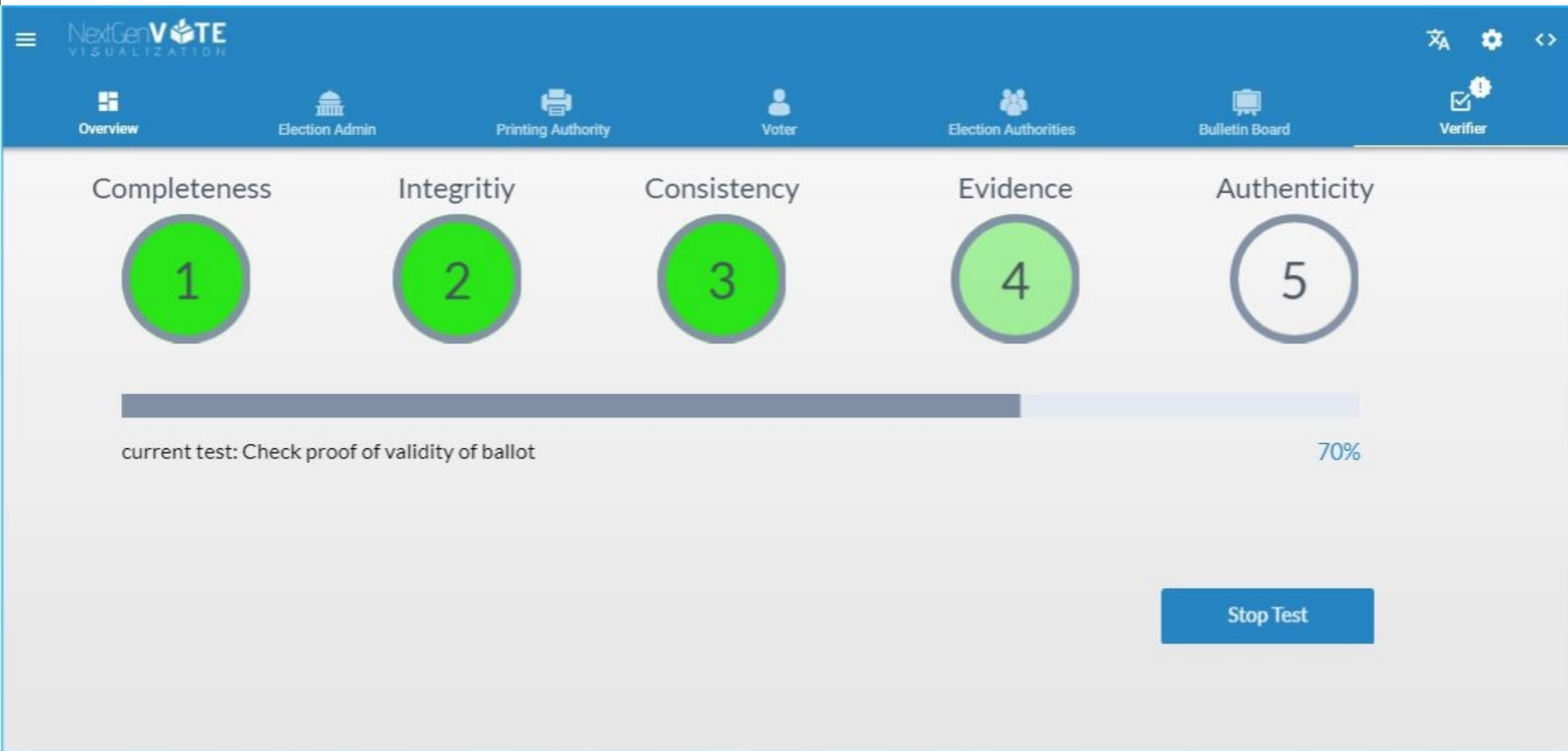
Authenticity



current test: Check if  $|n| = t$

50%

Stop Test



Completeness



Integrity



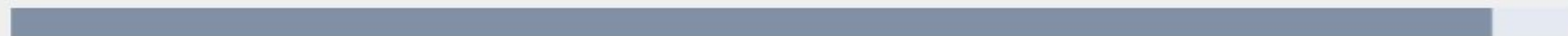
Consistency



Evidence



Authenticity



current test: Check signature of full election parameters

90%

Stop Test

Completeness



Integrity



Consistency



Evidence



Authenticity



Testing complete !

Click on the circle to get more informations

100%

Print Result as PDF

## Completeness



## Integrity



## Consistency



## Evidence

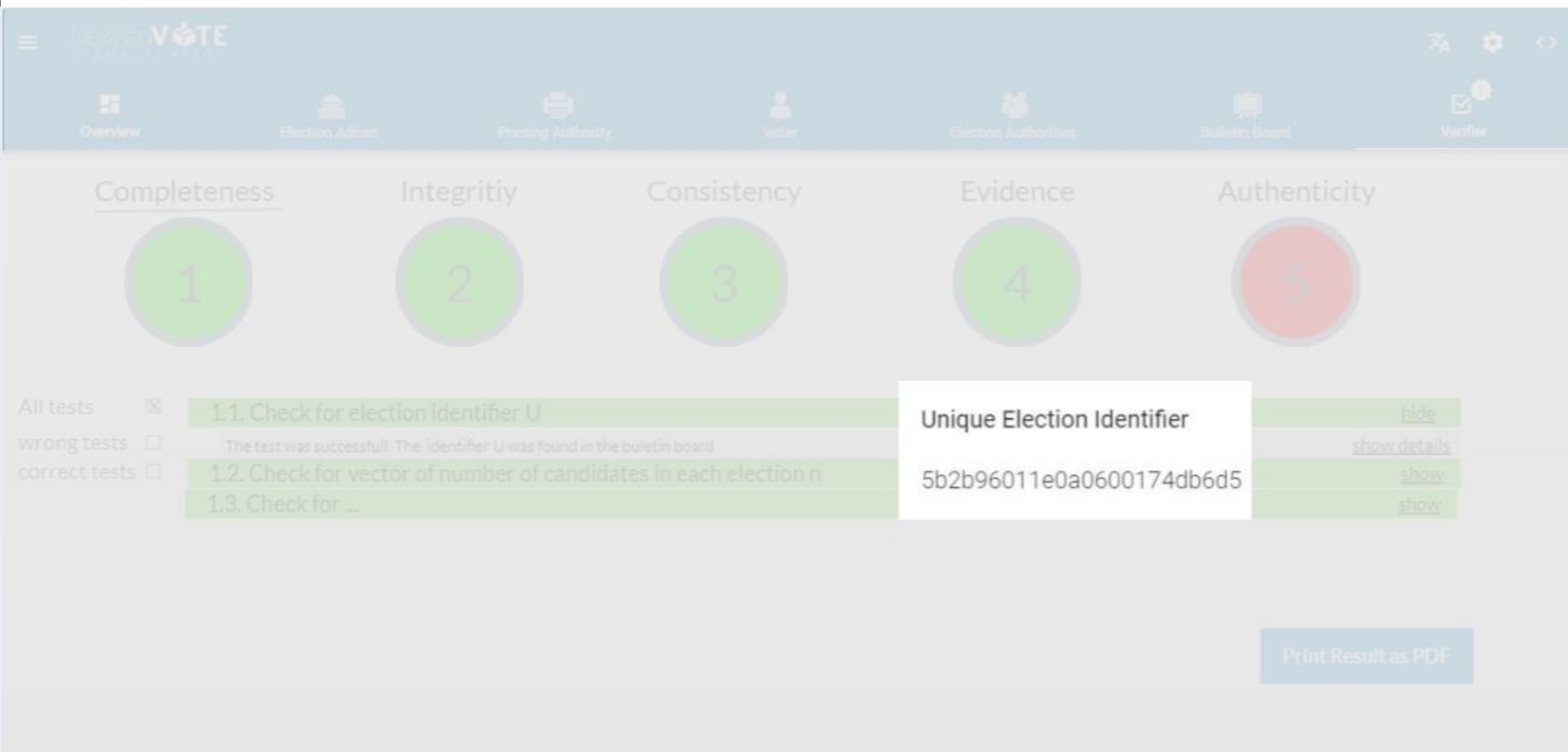


## Authenticity



All tests	<input checked="" type="checkbox"/>	1.1. Check for election identifier U	<a href="#">hide</a>
False tests	<input type="checkbox"/>	The test was successfull. The identifier U was found in the buletin	<a href="#">show details</a>
Correct tests	<input type="checkbox"/>	1.2. Check for vector of number of candidates in each election n	<a href="#">show</a>
		1.3. Check for ...	<a href="#">show</a>
		1.4. Check for ...	<a href="#">show</a>

Print Result as PDF



Completeness



Integrity



Consistency



Evidence



Authenticity

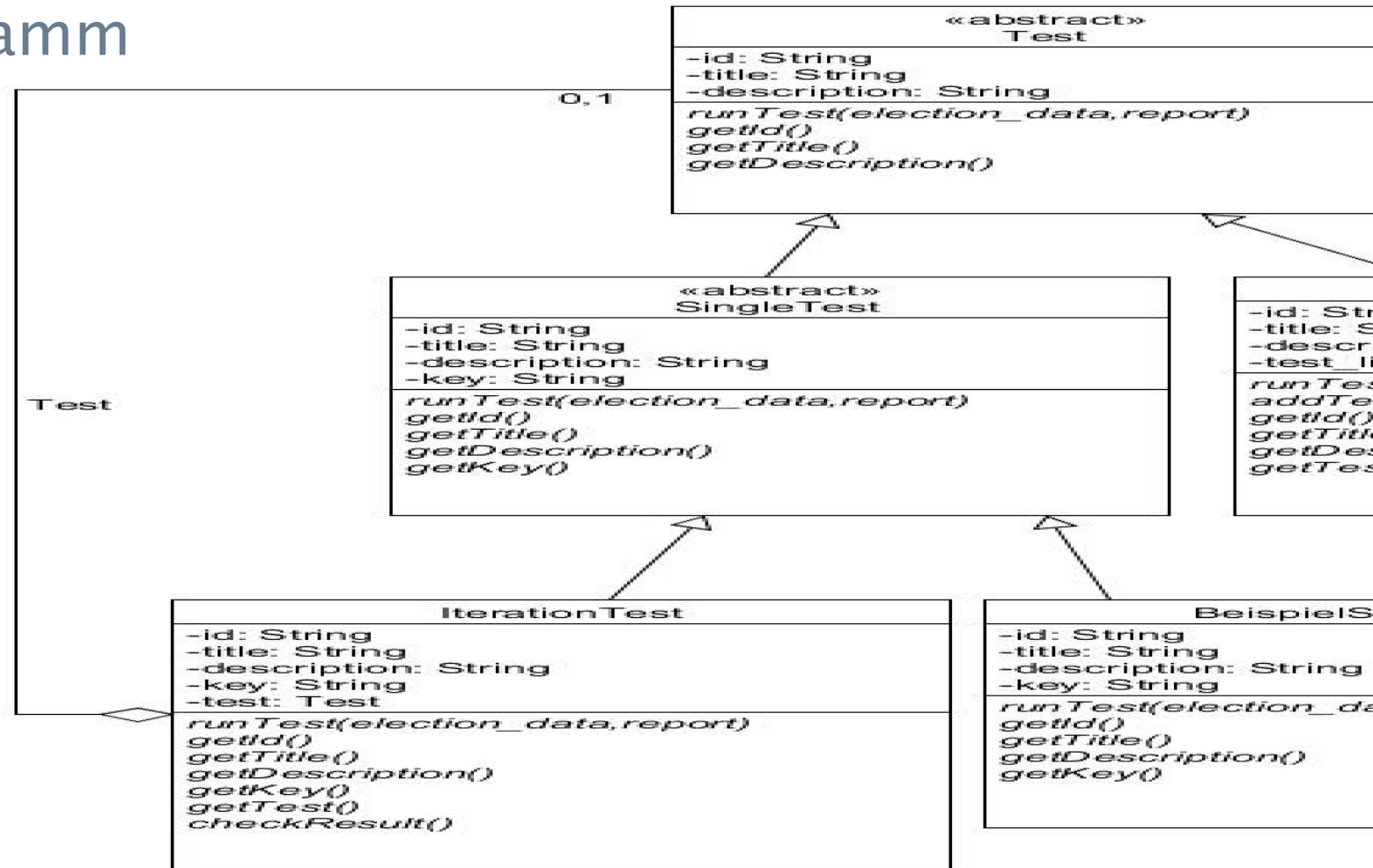


All tests	<input type="checkbox"/>	5.1. Check validity of Certificate of election administrator	<a href="#">hide</a>
wrong tests	<input checked="" type="checkbox"/>	The test was unsuccessful. The Certificate was not found !	<a href="#">show details</a>
correct tests	<input type="checkbox"/>	5.2. For all {1..s} check validity of the Certificates of election authorities	<a href="#">hide</a>
		5.2.1. Check Certificate of election authority 1	<a href="#">show</a>
		5.2.2. Check Certificate of election authority 2	<a href="#">show</a>
		5.2.3. Check Certificate of election authority ...	<a href="#">show</a>

Print Result as PDF



# Klassendiagramm



# Live Demo



Danke für Ihre Aufmerksamkeit.