

E-Voting EPFL : Authentication and Frontend

Etienne Bonvin

School of Computer and Communication Sciences
Decentralized and Distributed Systems lab

Semester project
Autumn 2017

Responsible
Prof. Bryan Ford
EPFL / DEDIS

Supervisor
Linus Gasser
EPFL / DEDIS

- 1 Introduction
- 2 Background
- 3 Implementation
 - Authentication server
 - Communication
 - Frontend
- 4 Limitations
- 5 Results
- 6 Conclusion

Introduction

and challenges



Privacy



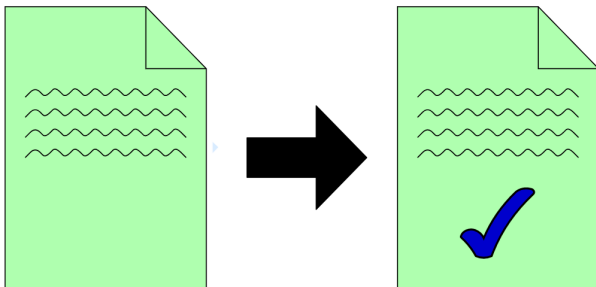
Authenticity



Reliability

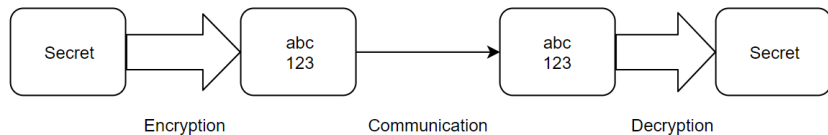
Schnorr Signature

an efficient identification scheme



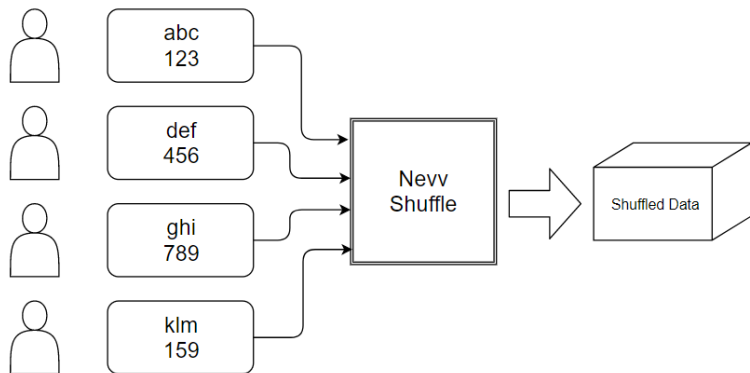
ElGamal Encryption System

asymmetric key encryption



Neff Shuffle

an insurance of privacy



Skipchains and Cothority

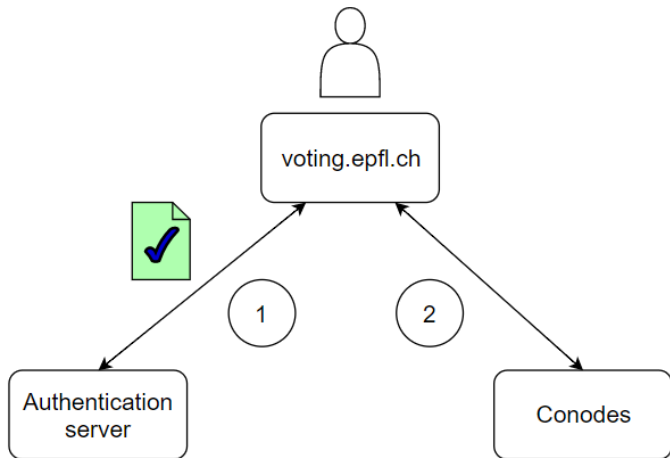
bringing reliability to the system

Cothority



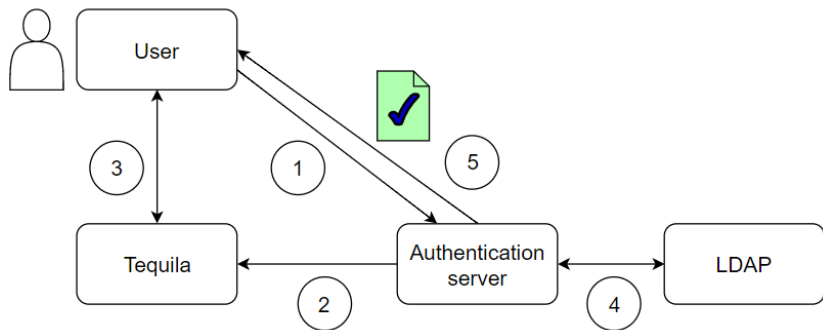
Authentication server

identify EPFL people



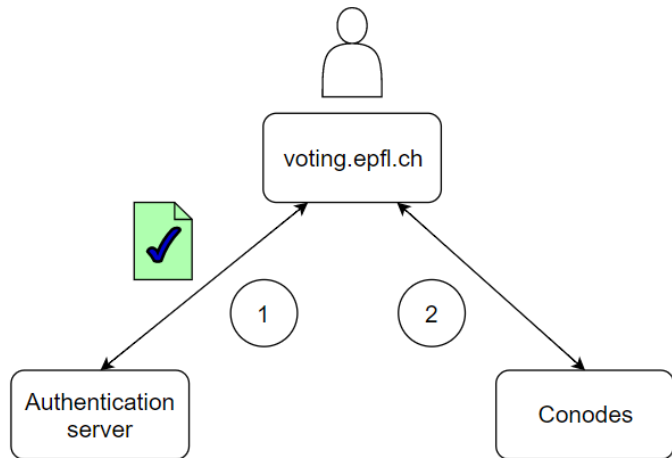
Authentication server

identify EPFL people



Communication

Frontend / Cothority



Communication

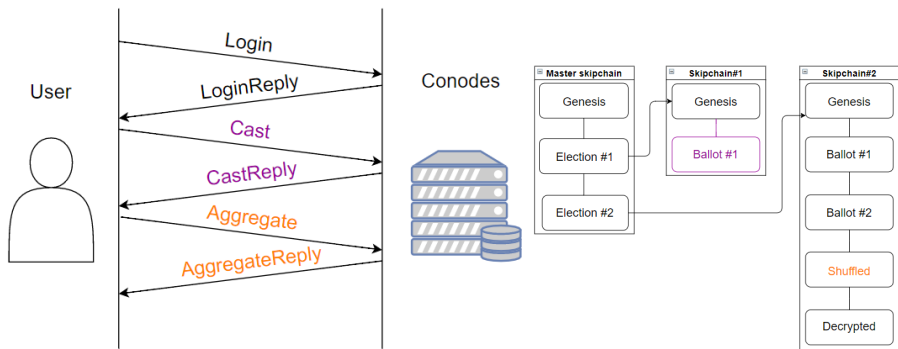
Frontend / Cothority

```
socket.send('Login', 'LoginReply', loginRequest).then((data) => {
  if(data.admin){ // The user is a confirmed admin.
    showConnectedScreen();
    sessionToken = data.token;
    displayElections(data.elections);
  }else{ // The user is not an admin.
    $("#errDiv").append(
      paragraph("An admin account is required "+
        "to access this site."));
  }
}).catch((err) => {
  displayError('An error occured during the login, "+
    "please try again later.');
```

```
  console.log(err);
});
```

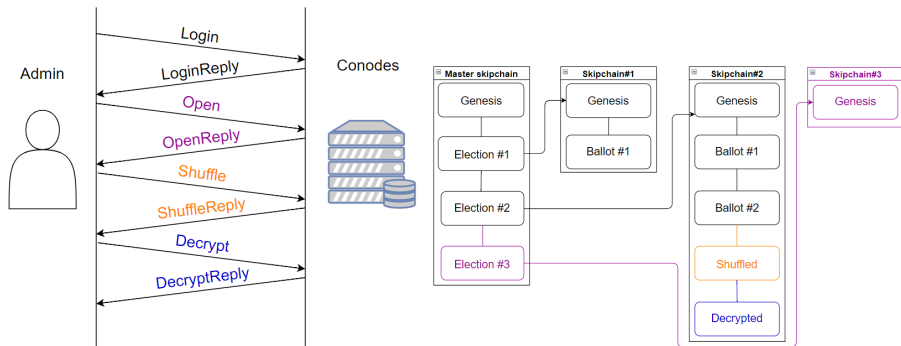
Communication

Frontend / Cothority











Communication

Frontend / Cothority



Frontend

communicate with the user

	User	Admin
Vote in election		
Create election		
Manage election		
See results		

Limitations

weak links and future enhancements

- **Nodejs server** : lose the no trusted server idea.
- **Authentication server message** : vulnerability to repetition attacks.
- **Elections limited to scipers**

Results

what has been achieved

Your ballot's encryption pair :

b29c9c202d905c37c35cdc1ad6336d2e34a9778e388044c555cb5517eb1fffd1
125c07ab786b1f841651c541fbb53528241e11e8fa377dba78a1b79b4a05d0e

Sciper	Alpha	Beta
100035	8a4d9e227eb13d39d310c59f2df4e2e0bfa6731d40840c45b9e0a1ac4ff5d	950f133428cce50d9af843a44629b1d6f16bc8bd359d27584fa81711a2ac2dc4
100019	a0815857d63362774a5fec3baa075039fe2b378447ab8be2d8d6f9bba63b6292	e720f1f894fa2e41f88f2a05adcfcded28e2665846904cc79465f66912d6a0c9
100025	970c2e225c824d3a4c1013cf28af75a759b835c1b479957f69ca42840c2f9ebb	9614ce52dae534b108078ec6336a1ee6a0738a2f4b1f74008825a54501ee0674
100042	2cf5fc7c6c06e1735e75862698e874338ee9765d8bcea12e7ff9dc5f156735b3	69eaf44ee824a04d1c31d3e0ce89aef1ed3c75ea008b4fc08beaadda979a9
100043	0d49dabcfb79bb5fc7c1491f13e2cb1d99e4ae33598aa74729d99626cd333678	785485e36acf66bb240a7c49380f9dbfb26c9792c663bf94068c0225e7a831d
100048	8f4e2cf999cb73140fadcd1d1ef29bc9ec2e552a21b0c91aa338058ea7cee982	c90e5a2ae8449877afb7452ba78956a7aa18818cc5d46a81d9c2e23adbc408e
100008	ca2faecd2a2f22f988a078e30a85823e1c6d9b1f861bb76c6435f010c4ee702e	aa86b8adde58c28ecbb17df2cd4f149bbd15a3d5cafe7cc372ea180a557224e
100013	9f6d42070389b5891a7569ce119bbcfeb2bf54986de4b6a392dd84a448f9bb	7f7aff125e964f5df0771c00a90ea972f367acbe5f1f602b67492e438550d33b
100016	defa79348d2290d9efc5eecddeb31132e14ad00e734110f535497c6d5493ca	46679c6cc5228f54896d24d9b77d75cd60cc388ce625a451633cbea960f77
100049	750fc7c7ad4073aec1e9852daa144f0a18a912b67d1754ef97a20adbe0b69c	ab83727df0045c5976dbf3c1c330c7a977f6f6120e0d48d5f6b5df94d59b708

9-19 of 45

Results

what has been achieved

Your shuffled ballot's encryption pair :

5954de2be853df67320621236b581bc3b4e2ade229976cc4c4f33927bf742989

97347646f61ee39315762b65a44b8a72ec23a8b6882cc9ca788188c7acbd1a86

Alpha	Beta
101dd9e8fbb5ab7ea3f1136663557b07dcd9feef8b8df5ba49ab28dc3509cd48	346e12f5378a07fe1263089f100bd8c94ec9a021914e913e36504913411d7d9
e6860c23972191f02636f8cc714e8cd1e1020b30c27342c6ef0554ddd5825f06	cc626745223504d05ac103fb78c79e3fd93dd7914dfe9d97d741ed756fc32731
db03c1d238bf7b7a146a36ab4ddcc59e0c89e283056128940d2a309330665ee9	38e197a9934d1b9491f00b06a64f8f69ea2bee683077f3fed2b1c48222dfc76
6b3b2069468855bf1fa842c447dd9a788d8ff011da8666e7894cb92e1293cf	6142c539c62756049eb9180dc3785c8d64bdc0c0bfaa610bf0ef06e0fafdaad
5954de2be853df67320621236b581bc3b4e2ade229976cc4c4f33927bf742989	97347646f61ee39315762b65a44b8a72ec23a8b6882cc9ca788188c7acbd1a86
3e43a5e2a39e50a61c4836b7dc97473db4eab8c6ff90a23b33aa80c5ae858904	f310c81cdc1d0a6210bc2a4c978fb1adab93bf25b6ccdf1589768378a8433d
8cc186f786993a05e6dd6727ed0f75806ed81bfcdef5cae3bec98b409ffa90	1bcdbdd5fa4c80b40203e3fcf1161287d6747c304822f61684f61a5ee3bd8c1
2b22d09971b90b2a0c8d84ba6a558c95ab34b439631946668fc53fff9e6cd01	231f92787cbccc44c87226fb01457dd1130d780ba5b6e7baae37df5fac4fbc4c
a486e41e4070d2a67c47677940fe481f367f9be9be90dd8b96d26032020323e	2aad297b4de6c8dbb6de11827a903623520bf3aa4b07242e8407cca178cc2faa
6a443e8b07f3161a47518e41a476b82524825b1c72e43e8190625719bd362a	7dc95d62911d2a995417e9d54608cccfb3a9781e9a46bbb8d3ce94ffb5463424
613838367da55acae5ca9da56e6a53656a985eb4bd6d009cad235dc8a2d391	d232596574370b63ee367c7212d7561d0906f1857b1e4cb2843d22cfdbd20c

Record ID: 19

16-26 of 45

Results

what has been achieved

Your vote : 456789

Place [▲]	Sciper	Votes
1	456789	10
2	123789	7
3	123456	6
4	248635	5

1-4 of 4

Conclusion

and future work

- Acknowledgments
- Future work

