Verifiable electronic voting in Norway
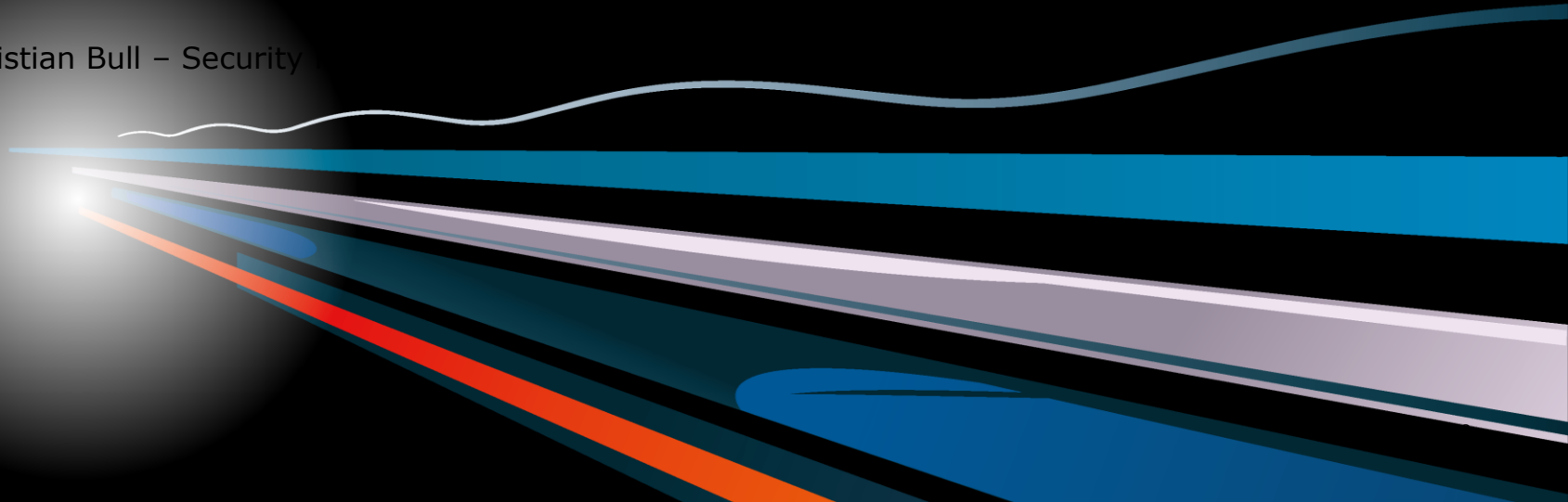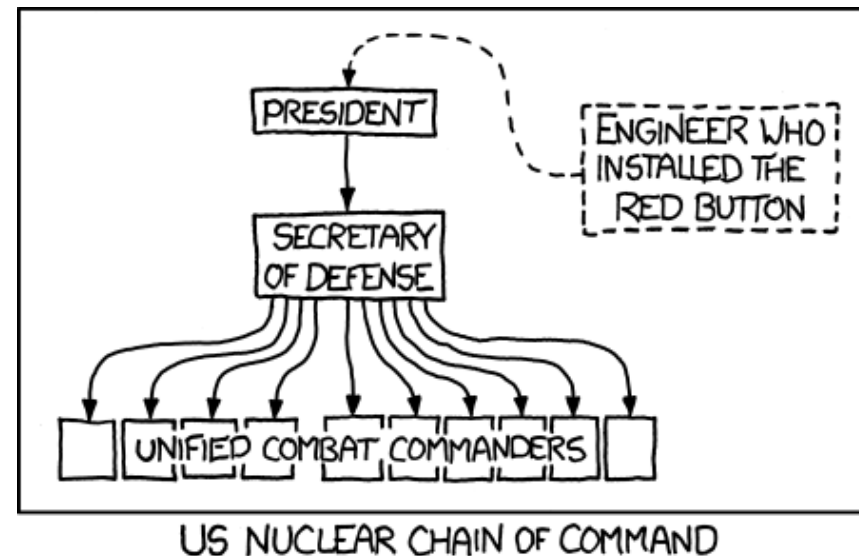
AFSecurity

Christian Bull – Security

What I'll be talking about

- Briefly about the pilot projects
- Even more briefly about the legal premises
- Security problems and our solutions to them
- The future of electronic voting in Norway

PRESIDENT

ENGINEER WHO INSTALLED THE RED BUTTON

SECRETARY OF DEFENSE

UNIFIED COMBAT COMMANDERS

US NUCLEAR CHAIN OF COMMAND

The e-vote 2011-project

- Initiated in August 2008, terminated in June 2012
  - Zombie-mode since then
- Project mandate to run limited trials with electronic voting
- Scope quickly swelled to administrative support system and scanning of paper ballots
- Electronic voting was hence a relatively minor part of the eventual scope
- Source code available, government owned, operated and developed

Why vote electronically?

Accessibility

You may think paper is perfect…

- Mistakes are made in reporting

- Interpreting voter intent is not always straightforward

- Paper gets lost
  - If you voted outside your municipality on september 6th, there was only a 95% chance that your vote would be counted

  - In total about 2% of mailed ballots are *lost* (about 0.23% of all ballots)

  - In comparison, exatly 0 e-votes were lost

E-voting and EVA

EVA – administrative support system

Electronic voting

Scanning of ballots

Legal premises

- Pilot provisions in Representation of The People Act make it possible to deviate from the law in trials

- …but not fundamental democratic principles.

- European Convention on Human Rights art. 3 requires secret suffrage
  - requires *certain measures* to be taken

10 pilot municipalities in 2011:

- Bodø
- Bremanger
- Hammerfest
- Mandal
- Radøy
- Re
- Tynset
- Vefsn
- Sandnes
- Ålesund
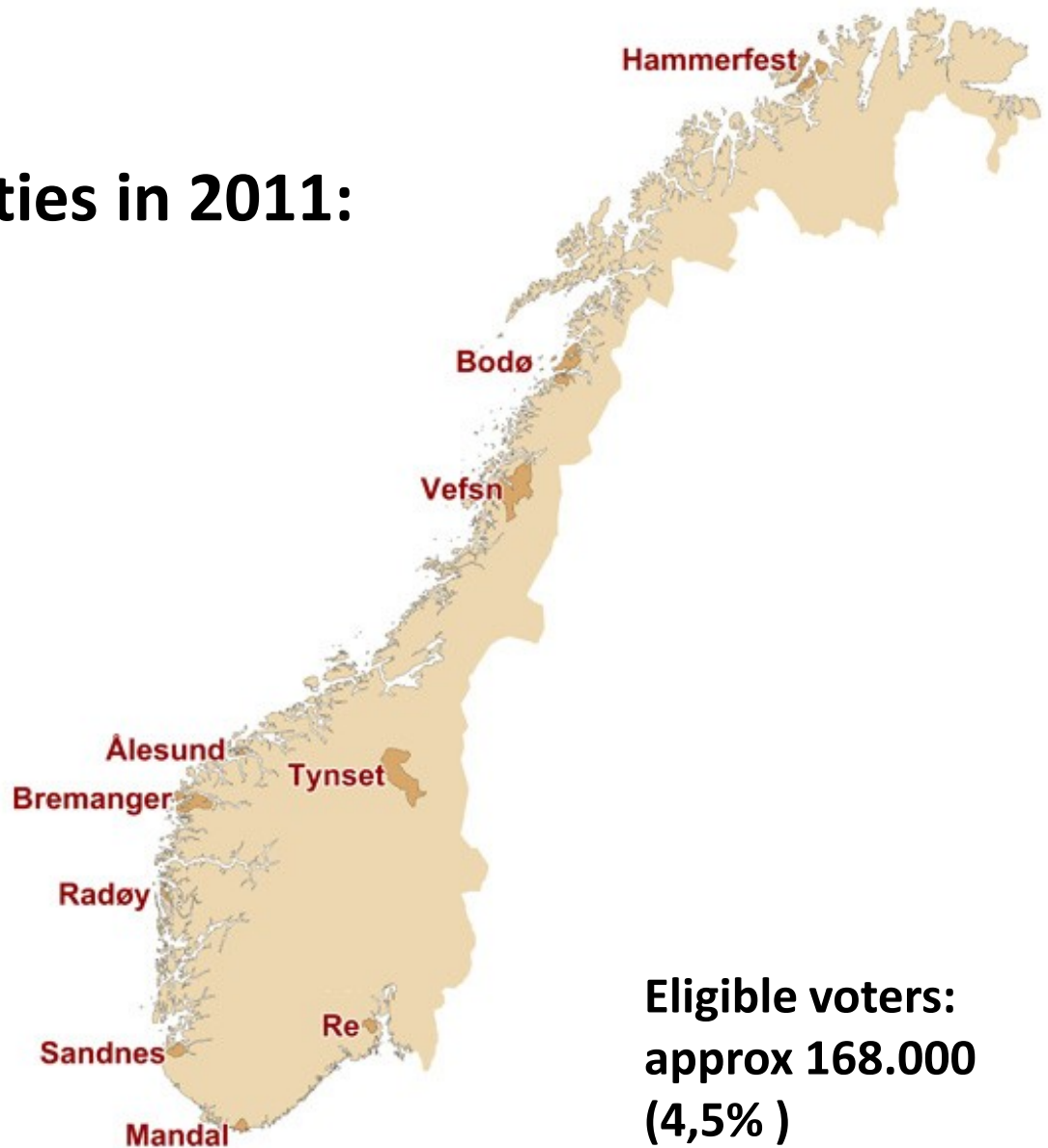
Eligible voters: approx 168.000 (4,5%)

How did it turn out?

- 28 001 voters out of approx. 168 000 eligible chose to cast their ballot over the Internet

- 73% of advance votes (26% of total) cast via Internet

- 15pp increase in advance voting

- 98% authenticated using MinID

- 92% of users happy with the solution

2013: Expansion of trials

- 2011 trials insufficient to answer all questions

- Apparently very successful – no cases of coercion or vote selling

- Need for experience over time, and to more closely examine «vulnerable groups»

- Added two further municipalities (Larvik and Fredrikstad) for a total of approx. 250.000 voters.

2013 results

- 2013: 70622 voters
- 76% of advance votes cast over the Internet
- 28% of total votes
- Under evaluation by ISF. Report to be published this summer.

VALG | Internet Voting TEST

The Norwegian Parliamentary Election 2013 TEST

English ▾

Internet voting

All eligible voters in Bodø, Bremanger, Fredrikstad, Hammerfest, Larvik, Mandal, Radøy, Re, Sandnes, Tynset, Vefsn og Ålesund may vote electronically during the parlamentary election.

You may vote online until September 6th 23:59.

For your security, you will automatically be logged out after 30 minutes.

How to vote online

Authentication is done through ID-porten (using, for example, MinID or BankID), where your cell phone number must be registered.

The first time you authenticate, you'll be prompted to share your phone number. **In order to vote online, you must select "Share with eValg".**

Watch a video illustrating the voting process.

Your ballot must be kept secret.

You must therfore ensure that you cast your vote unobserved.

Remember that you may vote via the Internet again at any time during the advance voting period. You may also vote with a paper ballot at a polling station. A paper vote will cancel an Internet vote.

Log in to vote   ❯

VALG | Internet Voting TEST

A **A** A

2013 parliamentary election

Your ballot must be kept secret

- You must therefore ensure that you cast your vote unobserved.

You may vote via the Internet as many times you want

- To vote again, you must log out and in again.
- In the interest of keeping the ballot secret, you will never be able to see previously cast votes.
- Your last Internet vote will be the one that counts.

A paper vote will cancel all Internet votes

- You may vote both via the Internet and on paper.
- You may only vote once on paper.
- On election day you may only vote at the polling station.

Parliamentary election in Hordaland
Online voting period: 1. January 2013 0:00:00 - 31. December 2013 23:59:00

Start voting

qa-evalg

VALG

Select an electronic ID:

MinID
MinID
Use codes from SMS or PIN code letter
>

bankID
BankID
Use security code generator from your bank
>

buypass
Buypass
Use smart card and card reader
>

COMMFIDES
Commfides
Use your USB stick
>

How to obtain an electronic ID

Contact form | Tel: 800 30 300 | Help to log in | Security and privacy

Operated by the Agency for Public Management and e-Government (Difi)

qa-evalg

VALG

Log in with MinID

MinID

Personal ID number:	211090	(11 digits)

Password:

Forgotten password?

CANCEL | NEXT →

Register as new user | Order PIN codes | Edit user profile

Contact form | Tel: 800 30 300 | Help to log in | Security and privacy

Operated by the Agency for Public Management and e-Government (Difi)

qa-evalg

VALG

Log in with MinID

MinID

Use PIN codes from letter dated **15.05.2013** .

Previous log-in: 27.09.2013 08:54

PIN code no. **4**: ●●●●● (5 digits)

CANCEL

NEXT ❯

Order PIN codes

VALG | Internet Voting TEST

A A A

Select ballot for parliamentary election in Hordaland

There are 15 electoral lists in your county. These are listed in random order below.
Choose the party you want to vote for.

- ○ Norges Kommunistiske Parti
- ○ Pensjonistpartiet
- ○ Det norske Arbeiderparti
- ○ Miljøpartiet De Grønne
- ○ Sentrumsalliansen
- ○ Rødt
- ○ Demokratene
- ○ Fremskrittspartiet
- ○ Sosialistisk Venstreparti
- ○ Kystpartiet
- ○ Venstre
- ○ Senterpartiet
- ○ Høyre
- ○ Kristent Samlingsparti
- ○ Kristelig Folkeparti

- ○ Blank stemmeseddel

Show ballot ›

VALG | Internet Voting TEST

A A **A**

Select ballot for parliamentary election in Hordaland

There are 15 electoral lists in your county. These are listed in random order below.
Choose the party you want to vote for.

- ● **Norges Kommunistiske Parti**
- ○ Pensjonistpartiet
- ○ Det norske Arbeiderparti
- ○ Miljøpartiet De Grønne
- ○ Sentrumsalliansen
- ○ Rødt
- ○ Demokratene
- ○ Fremskrittspartiet
- ○ Sosialistisk Venstreparti
- ○ Kystpartiet
- ○ Venstre
- ○ Senterpartiet
- ○ Høyre
- ○ Kristent Samlingsparti
- ○ Kristelig Folkeparti

- ○ Blank stemmeseddel

Show ballot ❯

 VALG | Internet Voting TEST

Ballot for Norges Kommunistiske Parti in the parliamentary election in Hordaland

You may change the sequence of the candidate list by entering new numbering in the boxes to the left of each candidate. You may also delete candidates by clicking in the field to the right of the candidate's name.

Change order

- Assign a new position to the candidate by clicking the associated field in front of the candidate's name and select the desired number from the list.
- You cannot assign multiple candidates to the same number.
- If you want to change the number of a candidate you have stricken, you must first uncheck the box to the right of the name.

Delete

- You may delete a candidate by checking the box to the right of the candidate.
- You may delete as many candidates as you want.
- In order to delete a candidate whose position you have reassigned, you must first remove the new number.

No	Change	Name	Birth year	Delete
1.		Benedikte Joakimsen	f. 1918	☐
2.		Idunn Kolbjørnsen	f. 1944	☐
3.		Angelina Austad	f. 1928	☐
4.		Mildrid Torgersen	f. 1952	☐
5.		Cecilie Tandstad	f. 1923	☐
6.		Håvard Endal	f. 1920	☐
7.		Bente Børsheim	f. 1970	☐
8.		Ruth Gjøsund	f. 1930	☐

VALG | Internet Voting TEST

A A **A**

Ballot for Norges Kommunistiske Parti in the parliamentary election in Hordaland

You may change the sequence of the candidate list by entering new numbering in the boxes to the left of each candidate. You may also delete candidates by clicking in the field to the right of the candidate's name.

Change order

- Assign a new position to the candidate by clicking the associated field in front of the candidate's name and select the desired number from the list.
- You cannot assign multiple candidates to the same number.
- If you want to change the number of a candidate you have stricken, you must first uncheck the box to the right of the name.

Delete

- You may delete a candidate by checking the box to the right of the candidate.
- You may delete as many candidates as you want.
- In order to delete a candidate whose position you have reassigned, you must first remove the new number.

No	Change	Name	Birth year	Delete
1.		Benedikte Joakimsen	f. 1918	☐

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16				

No	Change	Name	Birth year	Delete
2.		Idunn Kolbjørnsen	f. 1944	☐
3.		Angelina Austad	f. 1928	☐
4.		Mildrid Torgersen	f. 1952	☐
5.		Cecilie Tandstad	f. 1923	☐
6.		Håvard Endal	f. 1920	☐

VALG | Internet Voting TEST

A **A** A

Ballot for Norges Kommunistiske Parti in the parliamentary election in Hordaland

You may change the sequence of the candidate list by entering new numbering in the boxes to the left of each candidate. You may also delete candidates by clicking in the field to the right of the candidate's name.

Change order

- Assign a new position to the candidate by clicking the associated field in front of the candidate's name and select the desired number from the list.
- You cannot assign multiple candidates to the same number.
- If you want to change the number of a candidate you have stricken, you must first uncheck the box to the right of the name.

Delete

- You may delete a candidate by checking the box to the right of the candidate.
- You may delete as many candidates as you want.
- In order to delete a candidate whose position you have reassigned, you must first remove the new number.

No	Change	Name	Birth year	Delete
1.	5	Benedikte Joakimsen	f. 1918	
2.		Idunn Kolbjørnsen	f. 1944	☐
3.		Angelina Austad	f. 1928	☐
4.		Mildrid Torgersen	f. 1952	☐
5.		Cecilie Tandstad	f. 1923	☐
6.		Håvard Endal	f. 1920	☐
7.		Bente Børsheim	f. 1970	☐
8.		Ruth Gjøsund	f. 1930	☐

VALG | Internet Voting TEST

A A A

Ballot for Norges Kommunistiske Parti in the parliamentary election in Hordaland

You may change the sequence of the candidate list by entering new numbering in the boxes to the left of each candidate. You may also delete candidates by clicking in the field to the right of the candidate's name.

Change order
- Assign a new position to the candidate by clicking the associated field in front of the candidate's name and select the desired number from the list.
- You cannot assign multiple candidates to the same number.
- If you want to change the number of a candidate you have stricken, you must first uncheck the box to the right of the name.

Delete
- You may delete a candidate by checking the box to the right of the candidate.
- You may delete as many candidates as you want.
- In order to delete a candidate whose position you have reassigned, you must first remove the new number.

No	Change	Name	Birth year	Delete
1.	5	Benedikte Joakimsen	f. 1918	
2.		Idunn Kolbjørnsen	f. 1944	☐
3.		Angelina Austad	f. 1928	☑
4.		Mildrid Torgersen	f. 1952	☐
5.		Cecilie Tandstad	f. 1923	☑
6.		Håvard Endal	f. 1920	☐
7.		Bente Børsheim	f. 1970	☑
8.		Ruth Gjøsund	f. 1930	☐

VALG | Internet Voting TEST

Checking your ballot

Below you will find your completed ballot. If you have made changes to the ballot, these will be displayed. The rest of the candidate list will remain unchanged. Verify your ballot before submission.

You are voting for:

NORGES KOMMUNISTISKE PARTI

You have re-numbered the following candidates:

From	To	Name	Birth year
1	5	Benedikte Joakimsen	f. 1918

You have stricken the following candidates:

No	Name	Birth year
3	~~Angelina Austad~~	~~f. 1928~~
5	~~Cecilie Tandstad~~	~~f. 1923~~
7	~~Bente Børsheim~~	~~f. 1970~~
9	~~Viljar Løge~~	~~f. 1994~~
11	~~Sana Sjøen~~	~~f. 1968~~
13	~~Sanna Grønli~~	~~f. 1982~~
15	~~Siren Steiro~~	~~f. 1955~~

VALG | Internet Voting TEST

A A A

Your vote will now be recorded.
Please wait...
This normally takes between 15 and 60 seconds.

Casting an electronic ballot

Encryption

Signing
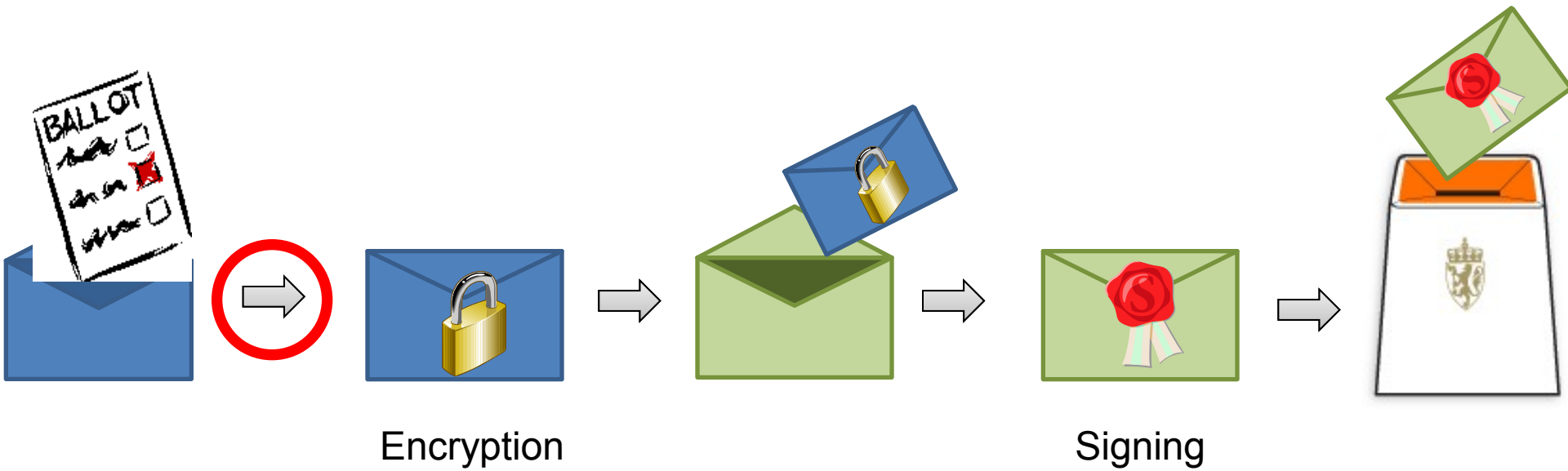
 VALG | Internet Voting TEST   A A **A**

Thank you for voting!

✓ **Your vote has now been recorded.**

- You will shortly receive a text message that contains a return code. This code allows you to verify that your vote has been registered correctly.
- Verify that the return code you receive in the text message is identical to the party/group's return code on your polling card. Each voter has a unique set of return codes.
- Please contact user support at 800 38 254 if the return codes received via text message and on the polling card do not match.

Do you want to help observe the Internet election?

Hei, din stem nottatt mo returkode re XXXX XXXX

Log out ❯

VALG | Internet Voting TEST

A A **A**

Find your vote in the digital ballot box

Your vote has now been submitted; this step is voluntary and not necessary in order to complete voting.

It may be advantageous to have a certain technical interest and insight to carry out this step, but in principle anyone can do it.

You can personally verify whether your vote has been saved in the digital ballot box. This will be possible until the votes are counted at the end of election day. By following the instructions on this page you can download an SHA-256 hash of your encrypted vote. It is important to understand that the hash does not reveal who you are or your vote.

A complete list of the hashes of all received votes will be published every hour on the hour at the GitHub page. The list will be updated and available until the votes are counted on election day. By checking that your hash is on the list, you will know that your Internet vote is saved in the digital ballot box. On election day, an independent third party will verify that the list matches the content of the digital ballot box when the contests are counted. As long as the list and ballot box match, we know all the votes are counted.

Please note!! If you navigate away from this page, you will not be able to see the hash of your encrypted vote later. You should therefore make sure that you save your hash.

See SHA-256 hash

Clicking the link below will display a hash and two digital signatures. The hash is an abbreviation of your encrypted vote. The signatures can be used to verify that the hash is from a real vote.

See the bullet point list below for a description of how to find your hash in the list.

- Click "See SHA-256 hash" below. This will bring up a screen with one hash and two hash signatures. You should save this information in an empty text document so you can look up your hash later.
- The list will be updated each hour. At the GitHub-page for the election you can find the textfile "Bulletin_130001.txt". When you open this textfile you can search for your hash, Ctrl+f, and paste in (Ctrl+v) your hash, to verify that your vote's hash is on the list. For a more detailed description of how to verify your vote see the "README"-file at the github-page.
- If you find the hash, you know that your vote has been received and stored.
- If you cannot find the hash, you may have been too quick and the list may not have been updated. If you believe the list has been updated after you voted, but you still cannot find your hash, call user support at 800 38 254.
- If you vote multiple times, all the hashes will be in the list. Feel free to verify multiple times.

Log out >

VALG | Int

A A A

SHA-256 hash av din krypterte stemme

Hash

n4RvpT88jqL7rPEbEh5VKCCEteexpMBqleSyunJRB48=

Hash signatures

PNv22sqnVlpmWC06Cf12amg+wLcXv2RQ63q6tkqDNTR7aJlHXVQKM3roW8ipSyHpr
tMzb/xnvnyY4A7Niw
/BufuVsHsd2+4RuTHZuruXXcyqVyz2iTsTzrWVMN0CKOlOWPBUpvTllGmV9+FeKjFu
V1FVLiLxlN3
/1y29hjXgdQBOkfULazrh72SKnGyrd4a+rsdFGwgtQlw7jzk8kFVV0BR5NR2ZcwbYFVft
bwPMLn1Fa8luHap1+KutCRiJ
/31zNHkKqxj17jwTxiXwvW7626ruBJJBfAsDTD5pUziQXJnHN5I8VW2C2Wh98ygYtA4
25/FhkcqDemnJBnvkc3Dfyw==

N7N4RSww+njsRIEF1VKI3/uSji9ncOXxSolQszXr6e0G/e0/1blXsEV2znuMb
/C63NecRE0lBq3RztCaF7vG85zTkwt9dl6hgDAZ5Jz9frEHWelHmsQw6Y4uzUVkQb7K
ifOeCvDJ+LOigtuzfijWabpcQUHSl9gJPUePyY4JNGGxo85xdD7s60XTnUdW0lJZYR1v
ulNd80wrijzJ+wXaQacA/kzkiGCD+49HmEmMueRsrFh7aulLVRDMhhMAVuQ8
/aOsnyFHJ1
/DiQrdDHkX0mmHxFj0onVP4YVmiHMQ1HwleeurFd4qR+aZ8W1MMUEDL3U7MH7cn
MBwn02RjDHgwA==

Close

Go to bulletin board

Hi, Erik Vik.

Your vote in the parliamentary election was received at 7/9-2013: 12:18.

The party/ group you voted for has return code 1758.

You deleted 7 candidates and made 1 re-numberings.

Please check the return code against your poll card. Call 800 38 254 if the return codes do not match.

Valgkort med returkoder

Stem via Internett på evalg.stat.no

1. Gå inn på evalg.stat.no
2. Gi din stemme
3. Kontroller at returkoden du får via SMS er den samme som på valgkortet

Hva bruker jeg returkodene som står på valgkortet til?

Returkodene på valgkortet er unike for deg og kan brukes til å kontrollere at stemmen din er kommet fram og er riktig registrert. Stemmer du via Internett, vil du få tilsendt en returkode via SMS. Returkoden kan du sammenligne med koden på valgkortet ditt. Kodene skal være like. Det er frivillig å gjøre denne kontrollen.

Hvis returkoden ikke er i samsvar med det du har stemt, er det viktig at vi får vite om det. Ta straks kontakt med brukerstøtte på tlf. 800 38 254 og meld fra om problemet.

0975

VALGKORT 2011
Kommunestyre- og fylkestingsvalget 2011

Bodø kommune
Valgstyret
Postboks 319
8001 Bodø

Nore Per Wessel
LANGHØYANE 28

0553 Forsøkskommune

Krets	Rode	Side	Linje
0025			

Fødselsår	Kommunenr.	Nr. i manntallet
1991	1804	000044

Navn	Nore Per Wessel

180400004411

Valglokale på valgdagen er:

Landego skole

8098 Landegode

På valgdagen er lokalet åpent:

16.08.2011 Kl. 11.00 - 05.00

Dato .... Stemmemottakers signatur
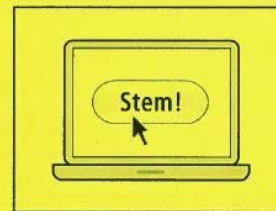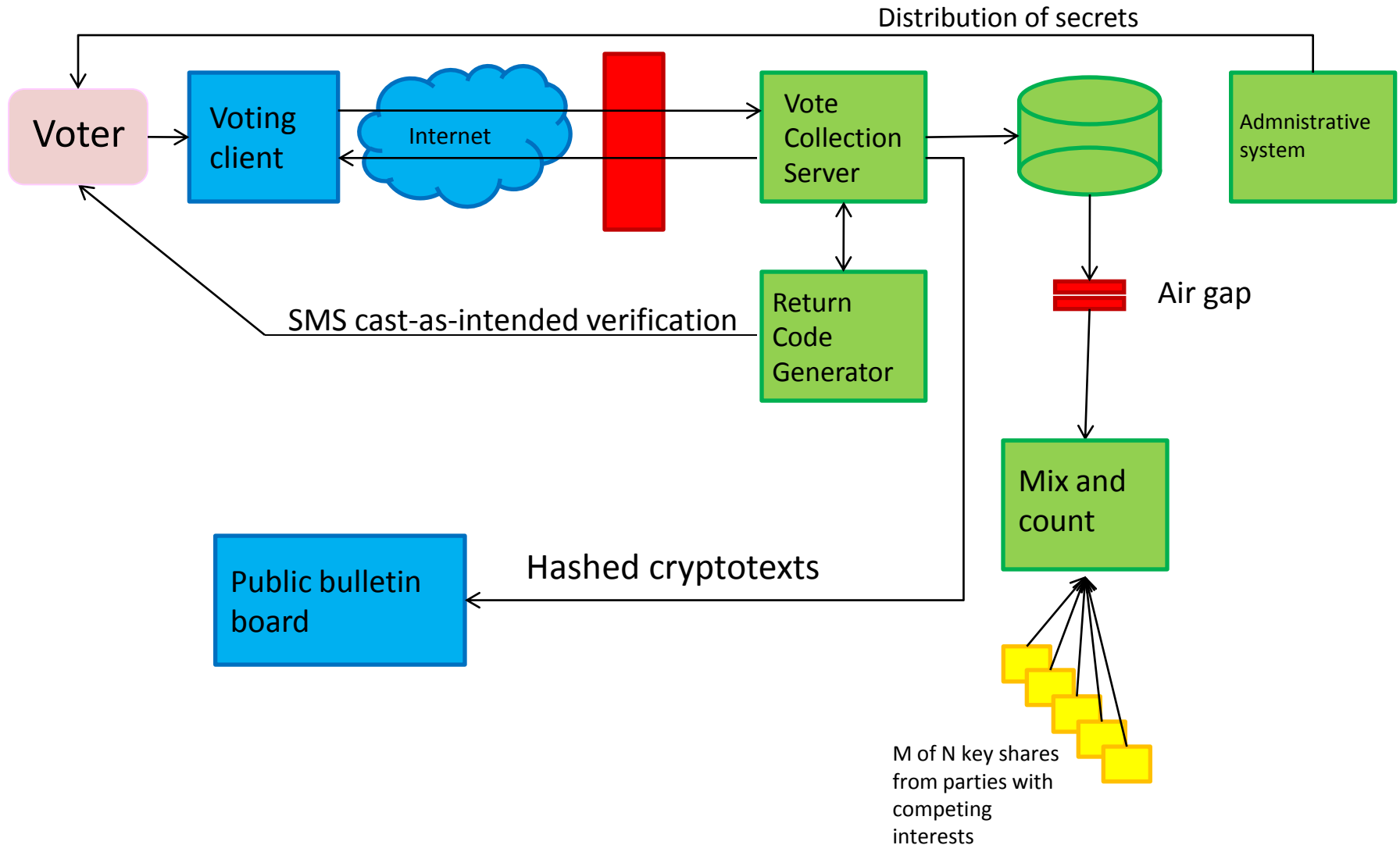
Returkoder for kommunestyre- og fylkestingsvalget

Parti- /gruppenavn	Kode	Parti- /gruppenavn	Kode
Blank stemmeseddel	6129	Det norske Arbeiderparti	3643
Demokratene i Norge	8152	Fremskrittspartiet	5766
Høyre	3605	Kristelig Folkeparti	0681
Kystpartiet	0975	Miljøpartiet De Grønne	7663
Norges Kommunistiske parti	2700	Pensjonistpartiet	5241
Rødt	5252	Samfunnspartiet	0321
Senterpartiet	3348	Sosialistisk Venstreparti	7153
Venstre	0904		

Ved valg skal alle få stemme på det partiet eller den gruppen de selv ønsker. Pass derfor på at du er alene når du stemmer via Internett, og at ingen andre ser hva du stemmer på. Husk at du når som helst kan stemme på nytt, både i forhåndsstemmeperioden og på valgdagen. På valgdagen må du gå i et valglokale og stemme der.
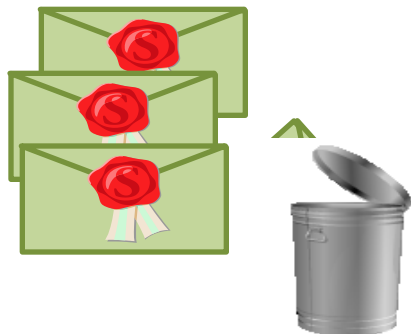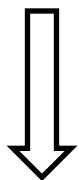
Revised conceptual model

Distribution of secrets

Voter

Voting client

Internet

Vote Collection Server

Admnistrative system

Return Code Generator

SMS cast-as-intended verification

Air gap

Mix and count

Public bulletin board

Hashed cryptotexts
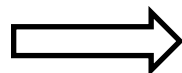
M of N key shares from parties with competing interests
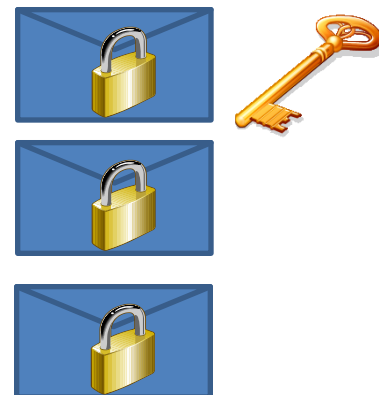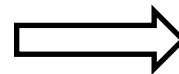
Counting process

Electronic ballots

Cleansing

Mixing

Decryption

Result

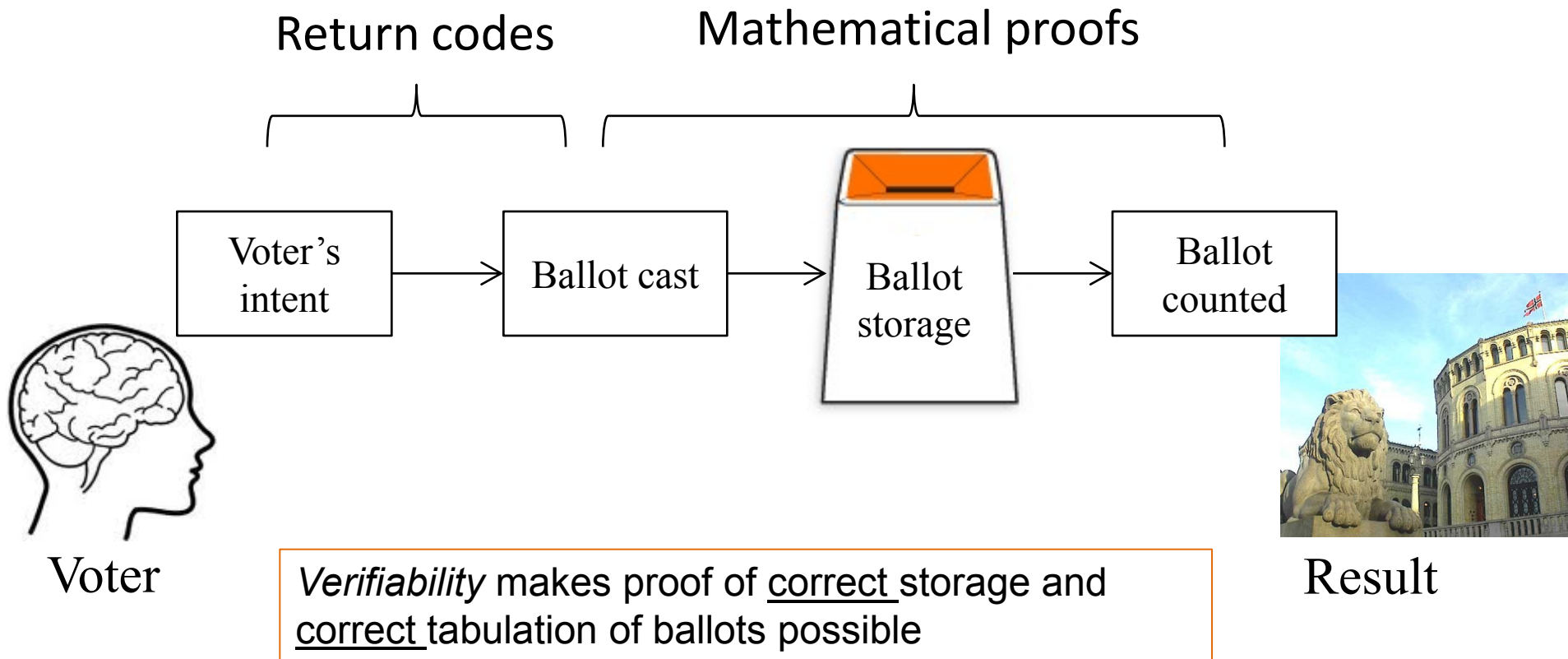# Observation of paper voting
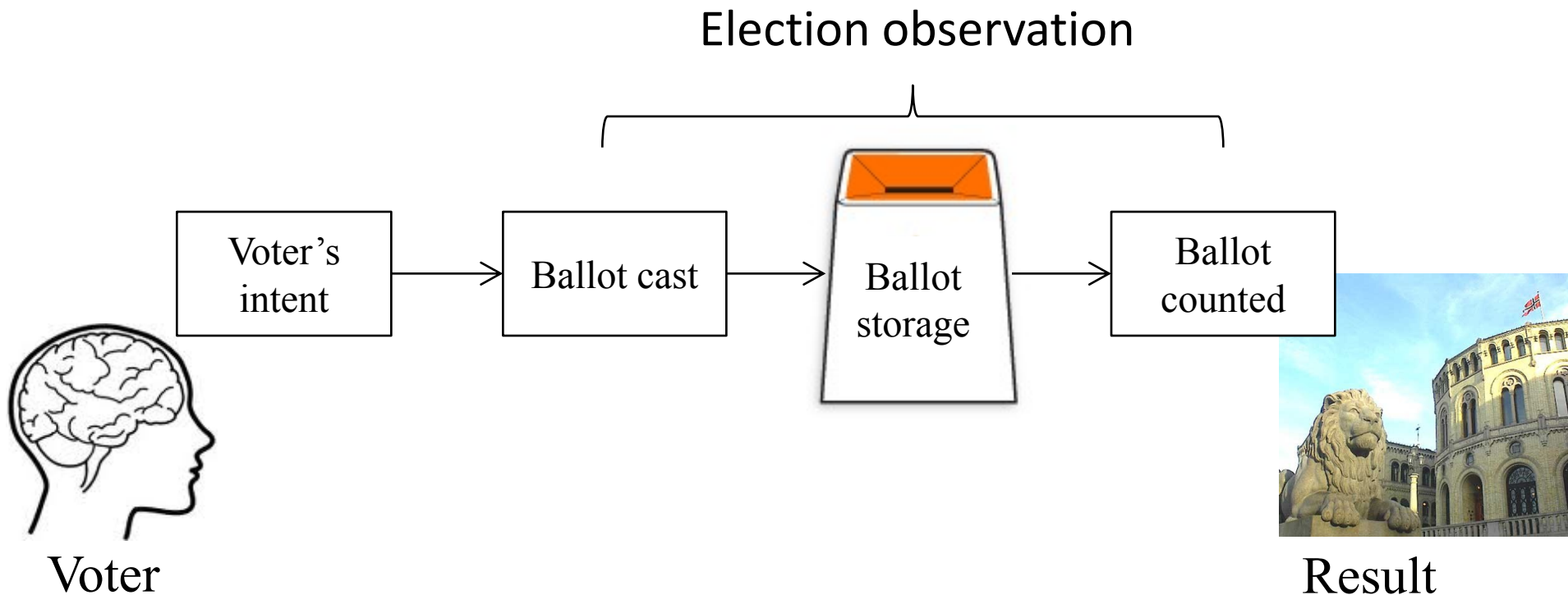
Observation of electronic voting

Return codes

Mathematical proofs

Voter's intent → Ballot cast → Ballot storage → Ballot counted

Voter

Result

Verifiability makes proof of <u>correct</u> storage and <u>correct</u> tabulation of ballots possible

The future?

- In the near term the future of internet voting is highly uncertain.

- Høyre and FrP have expressed very negative opinions

- Short term there may be more of an appetite for e-voting in the polling station.

Authentication woes

- At «levels» 3 and 4 we have pretty much the same degree of certainty about the identity of the voter

- The biggest problem is probably not us not knowing who the user is, but if the user knows what service he's authenticating to

- If we have authentication mechanisms that are highly vulnerable to phishing, that's *not* ok.

- This is the case with mechanisms in place today.

- We need a secure channel back to the voter. SMS is not that channel in the future.

An example of a solution: Cronto