ÞJÓNUSTA FYRIR ÞIG

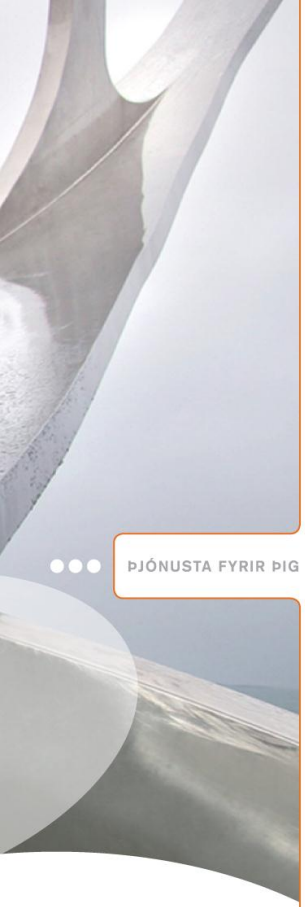
Betri Reykjavík

REYKJAVÍKURBORG

Rafrænar kosningar
Tæknileg framkvæmd

Erindi flutt hjá Ský, 23. maí 2012

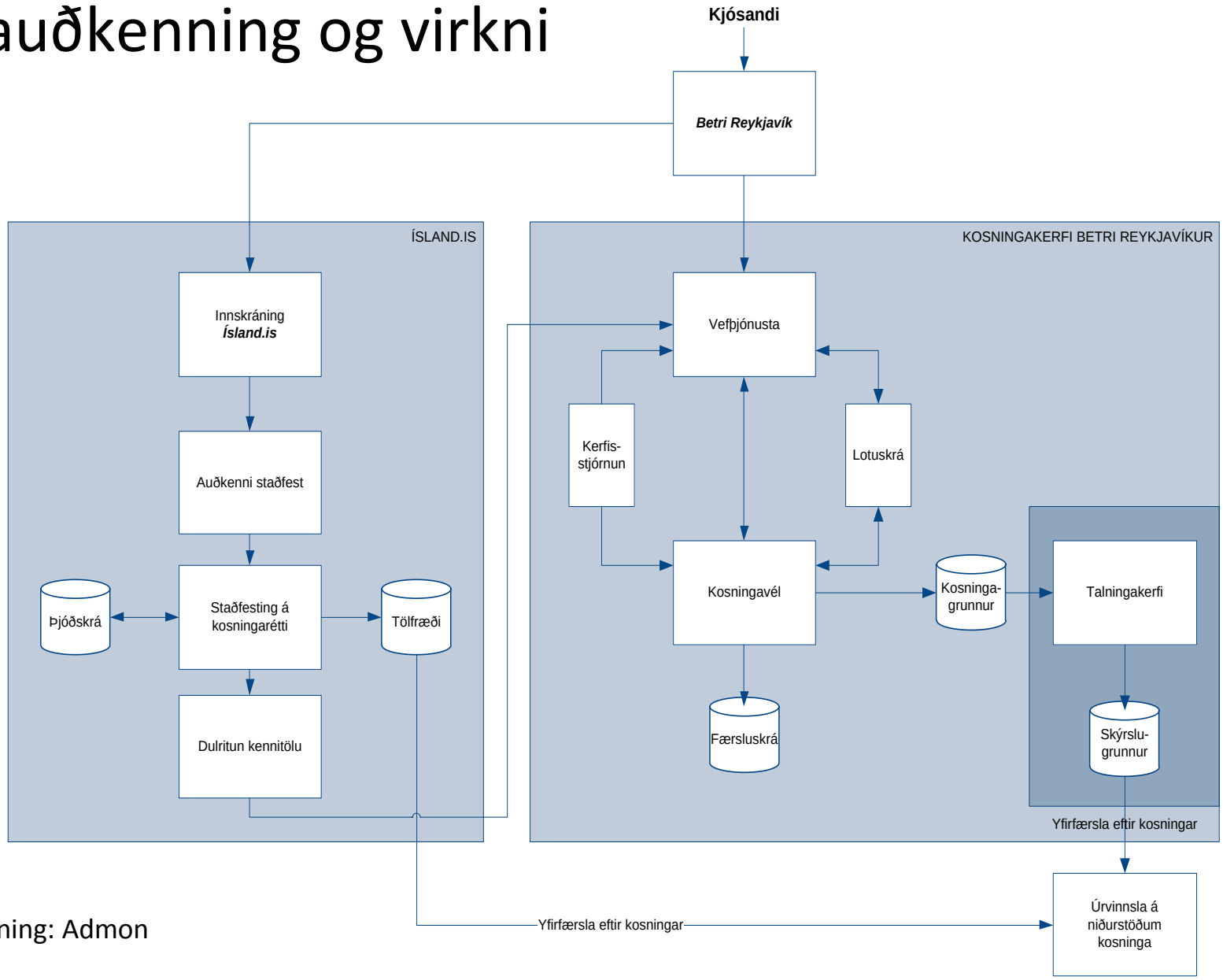
Eggert Ólafsson
Upplýsingatæknimiðstöð Reykjavíkurborgar - UTM



Yfirlit

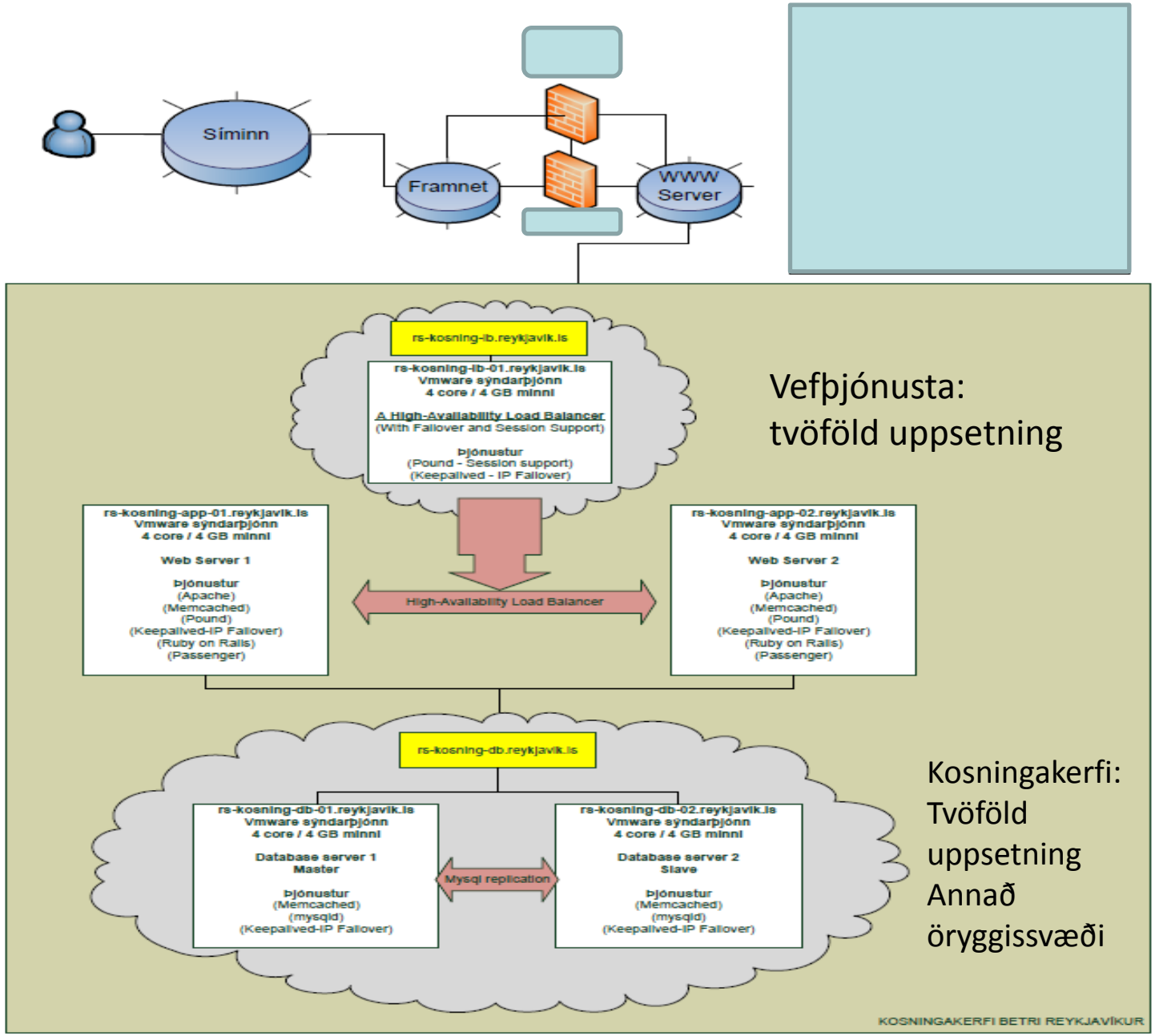
- Kosningakerfið
  - Auðkenning og virkni
  - Kerfishögun hjá UTM
  - Virknirit
- Öryggisráðstafanir
  - Lyklar og læsingar
  - Aðgangsheimildir
  - Talningar
- Prófanir
- Úttekt og lærdómar

Kosningakerfið – auðkenning og virkni



Teikning: Admon

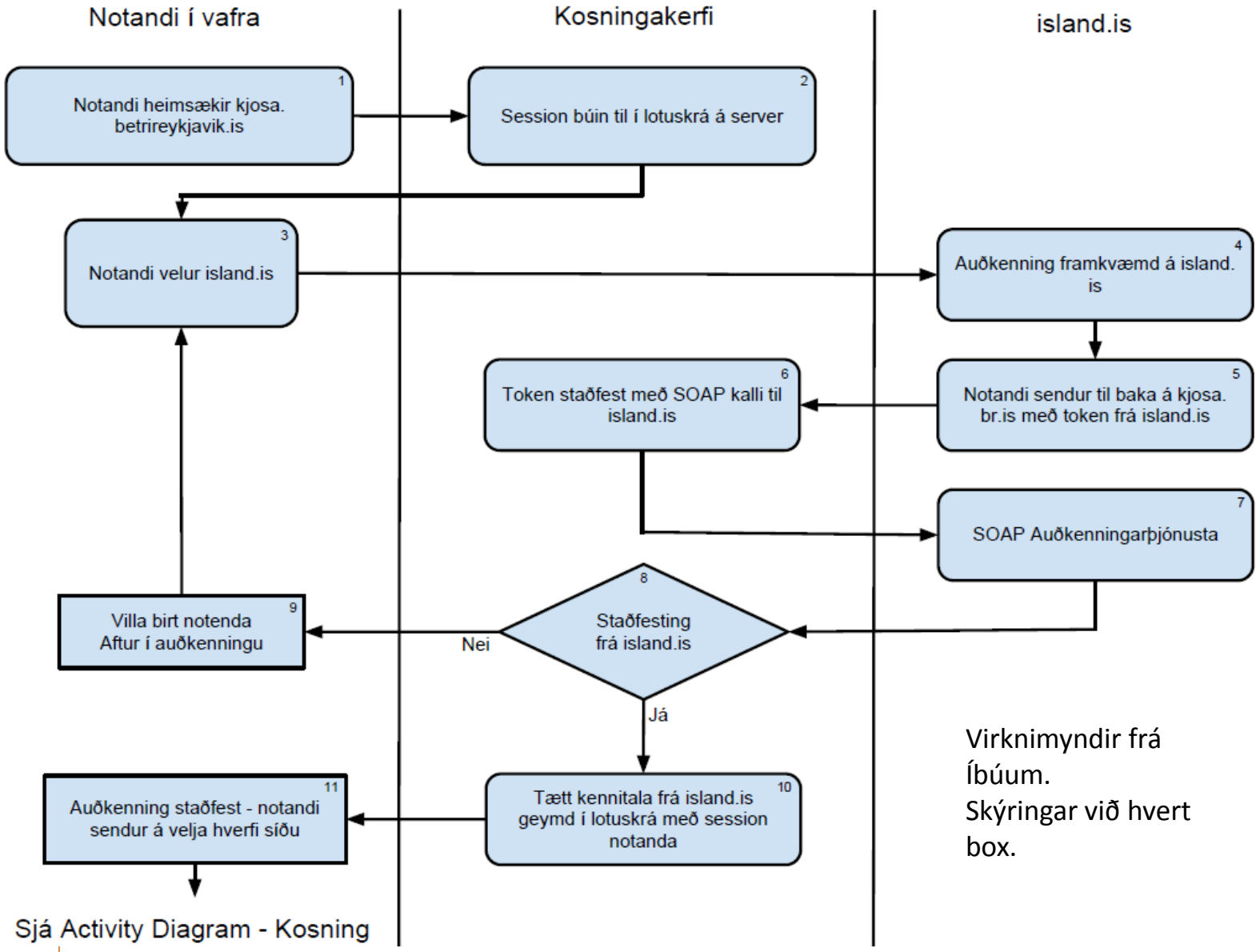
Kerfishögun kosningakerfis hjá UTM



Vefþjónusta:
tvöföld uppsetning

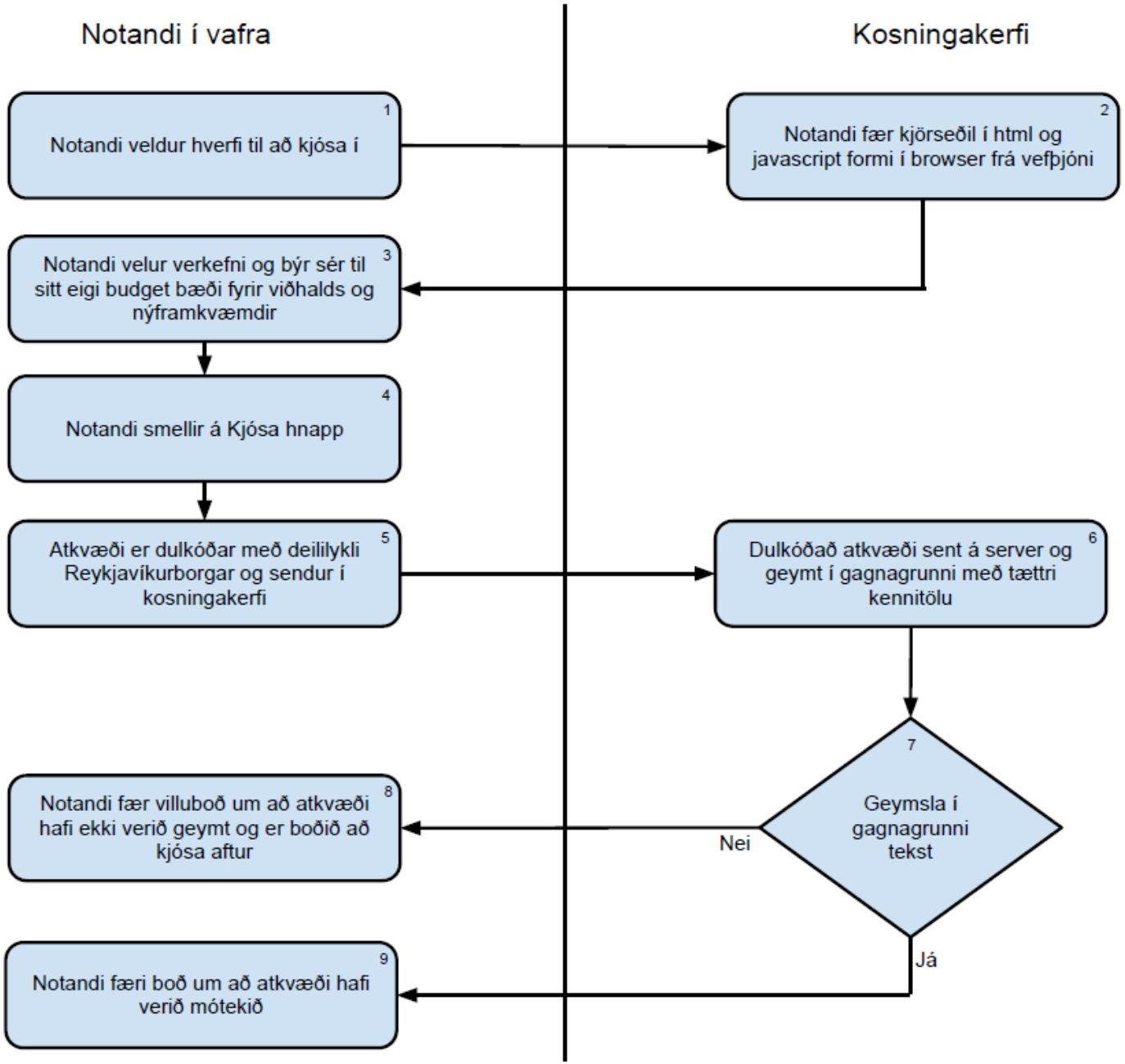
Kosningakerfi:
Tvöföld
uppsetning
Annað
öryggissvæði

Activity Diagram - Auðkenning

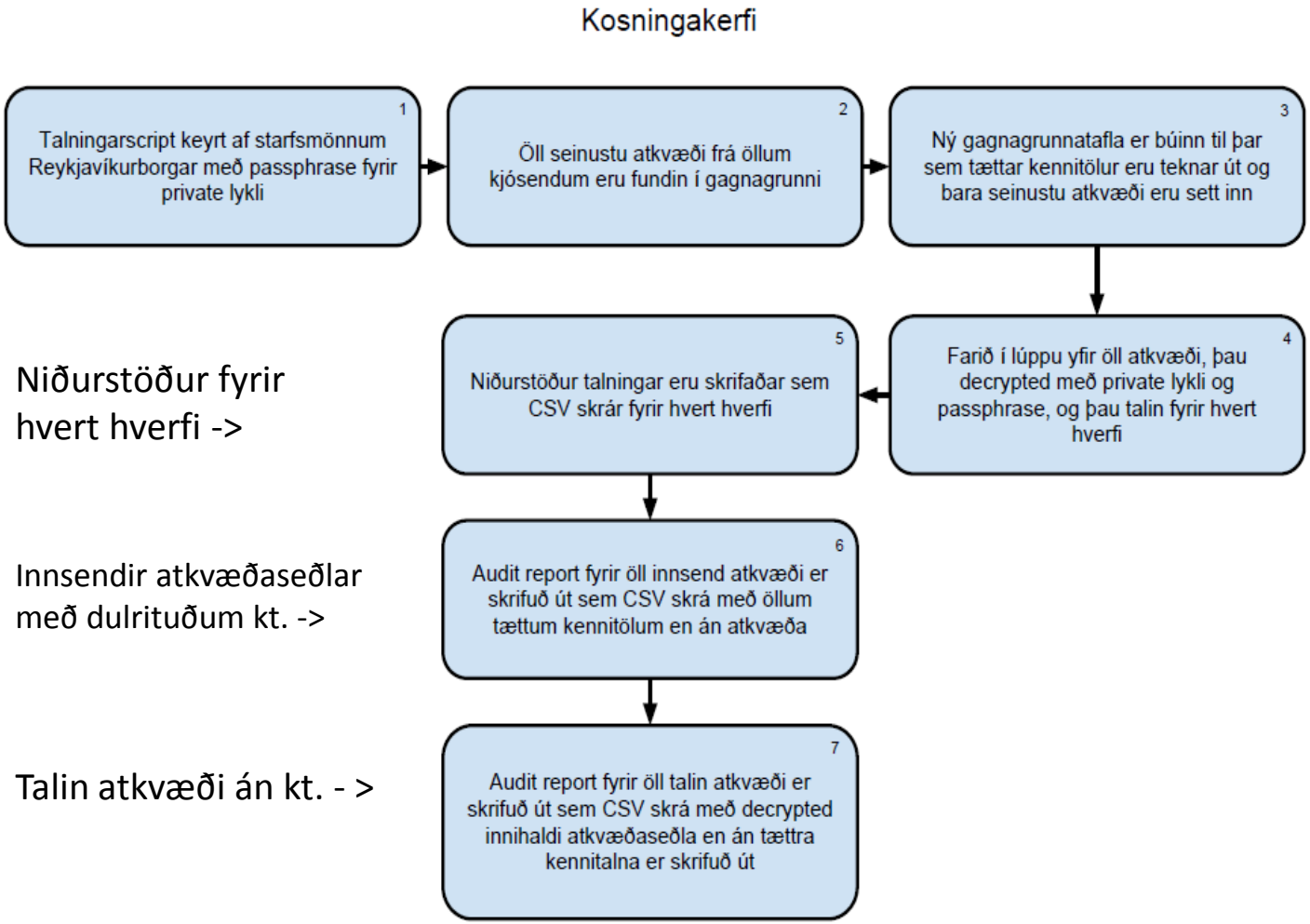


Virknimyndir frá Íbúum.
Skýringar við hvert box.

Activity Diagram - Kosning



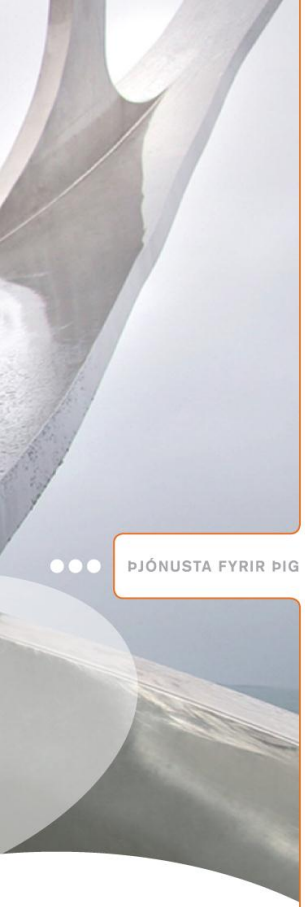
Activity Diagram - Talning



Niðurstöður fyrir hvert hverfi ->

Innsendir atkvæðaseðlar með dulrituðum kt. ->

Talin atkvæði án kt. - >



Öryggisráðstafanir: Lyklar og læsingar

- RSA 2048 bita lyklapar (dreifilykill/einkalykill)
- Atkvæði o.fl. dulritуð með dreifilykli
- Aðeins hægt að opna kjörkassa og sjá atkvæði með einkalykli
- Einkalykill í tvíriti, rafrænn (USB) og á pappír

Einkalykill útprentaður

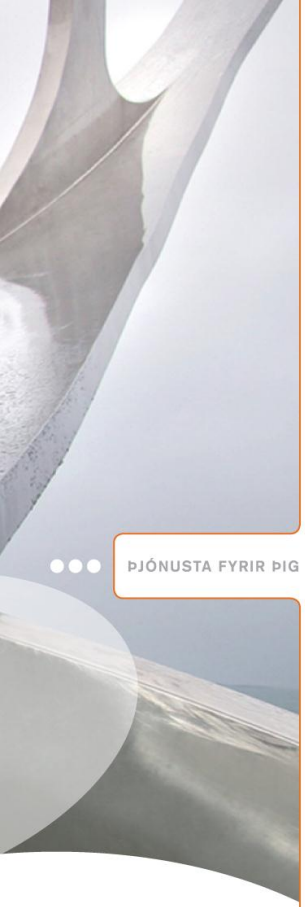
-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,67FB999D5BC52C8A

T75uUbgQRSiWGA64ViJMoKZenUuUIrdZ3axRf/sf54tfc1HHpk4DAUHFUwWdf+4p1xKk7/6niyDY2rBpHT83Gn
G6ZPKcsSDQhz2UDNZNJWMzRSKJxhMTNhqrp8TgjK0Bol6tcs60ZZSFJk+TVQplcMq7WkkxKm/WXjBVoAIF2qT
5Ccj+c19E85W0ixvSkwP8r4YPf94Dt/C1Kva4sENKH8f5+7yGx160p32tbmAogGfKOCMLjyBPXgJukgQVNNYyrR
0Ytc5KrX7RS8sEtdKTS4vLNqo1r3REJxbYk1QiT9G2NaEtzljErsS21ZnJkH+gFmg4quVYkI4jbPIll/ip0KJwevNtpiO4
dl7XbUEB9zDw+/FfrmYOLFxxLf+3A40PxOKVTvsnS9WccqHXxdblXp/5ZveJCf4Vgn/6aGwlnR736pa3wZiHdKyu
AnBg5LzqwJ4BGbvAskSCO/HuPysBwcrD2oviFuk2Ygd35lA55HV8hlVrjdTXVu41Ua57tx5HoIh7eW9rM9/pgwv
17MBAtQxnJVj1PDI7boc+cpRhxWi2yrn6Sn9IjNXsWR2tRDsjy/fLpjyezvj9MlL8tyOcqrOX6N6oJLvXK44Iq0Q5yC
uJ1qSTOG1eutkQnFqCpJp+ZcVCOq7+IlsojYPRjRi6fLowSgXpQFijoCAwXH5z7BpconVT8ZaJwtzzslM0qHTQkjLf
yCWmRGSgC0qbv9WwPi+tOEYrD1P3ynMrUYGxEtY0W0teVKl0wdOiVo9r+H2jR3wEmo+wgyxH/NQeD/b9px
czC3adWMf9eW7U9rqbCgnN5vMiJ3vimA/M25i9ftIOuweUpJNnFq76qVuWtXf3K+O5+xGuFZzk7Xc7ToSITtN
Ocob2p8kn31LXaoWFzi47qnMPzLpgi8Gs2y+0xccf3jm6Vvc73uRE1amVCUR7iG8+M2bZKXZLqxevz87Q2yXuy
+tZMIF4X9Ik2NjJ3KG6R+9cy1UP2OqOEE516xkoS1VY7kQ6aE//oTsFRgfzLGOEgAk3/Asb4RZC4OD7e787owZR
Q7O68xauSf3jmTt+JoMGZ1E7SnSsZzd/WRFf+p4Z6lx55DXRvJ9m6X+gqz3oWsLdBE2q2Qgu5v4iADlBJU5+fby
OplySMR8Uj1rdIdtIgKn/QJbb5Rr+Iv6IN+cVmlDKbF5+YvJjrfx+mTqgi3NYHCNMJrj9nFiPPt+ETiuAKQNII/S88M+
3XjL0msSAQhiAtiiHYOBg1ZAQUUcPGe27vwU9ZQja4zslpAC9J6/6+TPX5u2YPsTEfBNUmUawG6bWgPpUR1W
Lw9nic+Axxb43eEeMZeKF73Jvdu/K8ZuutJMNEjYlT4ElBJncNse0FjHDAeKGCo5a9SYWX8a3pr2j5LJJzYORCyYfk
sTAkqKqyp5o8TFM/hl7sJkCzOTQSTJRemKyuVIJQf/Q8FB4+dgTqurGR7i4Q5B0JSS+WOhP0hR7Bls9aDA4uMG
yQCECybk4CYlyOYkg/yBIszjyX6C1VClokKcf8C+fBnPux97dlTmdniE2yeWxtwezR1UJTSXvXSsd5QVgYQIZHjOq
Wgxz0kbwEYlS/jfJc3qCYcPj

-----END RSA PRIVATE KEY-----



Verndun einkalykilsins

- Vistaður í tveimur öryggishólfum
- Aðeins virkjaður með 12 stafa flóknu lykilorði
- Hálft lykilorð hjá borgarritara og í öryggishólfi í innsigluðu umslagi
- Hálft hjá borgarlögmanni og í öðru öryggishólfi sem aðrir höfðu aðgang að
- Urðu báðar að mæta

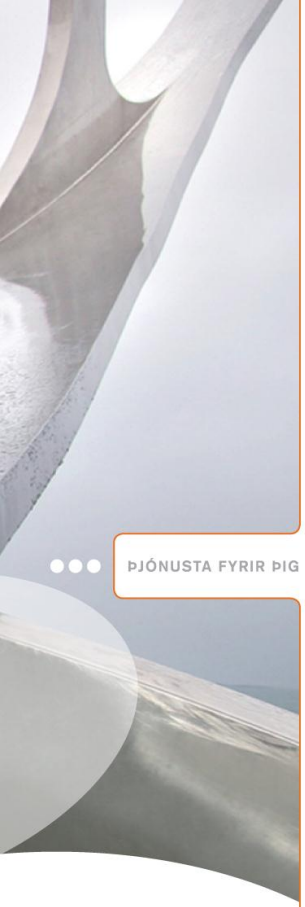
Aðgangsheimildir

það má eyðileggja allar kosningar með samsæri

- Þrír kerfisstjórar UTM með aðgang að netjónum kosningakerfis
- Einn sérfræðingur verktaka (ekki Íbúa) með takmarkaðan aðgang – setti upp kosningakerfið
- Öryggissérfræðingur UTM með aðgang að öðru öryggishólfi, en ekki að kosningakerfi
- Innri endurskoðandi með aðgang að hinu öryggishólfinu
- Borgarritari með hálft lykilorð
- Borgarlögmaður með hálft lykilorð
- Þjóðskrá Íslands með kennitölur kjósenda, R-borg aðeins með þær dulritaðar
- Úttektaraðili með aðgang að kóða kosningakerfis, fyrir og eftir kosningar, summutölum o.fl. til þess að rýna kóða og sannreyna að engu hafi verið breytt

Talning

- Sérstök Linux-vél til þess að virkja einkalykil og sjá um talningu atkvæða
  - Sett upp undir eftirliti öryggissérfræðings UTM
  - Stýrikerfið geymt á USB-lykli
  - Aldrei notuð til annars
  - Aldrei tengd við net nema við prófanir og í talningu
  - Aðeins opið inn á þessa einu vél frá kosningakerfi
  - Öll samskipti dulrituð

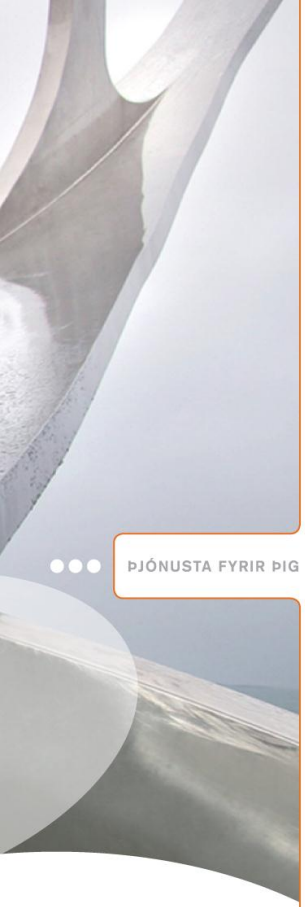


Prófanir

- Álagsprófanir:
  - 50 kjósendur kusu viðstöðulaust
  - Flöskuhálsar komu í ljós – var lagað
- Opin prófun:
  - 100 starfsmenn borgarinnar kusu að vild
  - Borið saman við tölur frá island.is
- Lokuð prófun:
  - 12 útvaldir kusu eftir forskrift
  - allt ferlið prófað
  - talið handvirkt og borið saman

Úttekt

- Admon fylgdist með verkefninu og gerði úttekt
- Ýmsar ábendingar sem komu að gagni
  - Verndun atkvæða og öryggi atkvæðagreiðslu
  - Nákvæmari virknirit og meiri skjölun
- Meginniðurstaða að kosningakerfið og tæknileg útfærsla hafi verið ásættanlegt
- Verkefnið mjög gott skref í þróun rafrænna kosninga
- Úttektarskýrsla enn í vinnslu



Lærdómar og álitamál

- Skilgreina betur öryggiskröfur?
- Skjala kerfi og vinnu betur?
- Tengingar við Facebook og Google?
  - Tvöfalt gler eða þrefalt?
- Fleiri auðkenningarleiðir?
- Öflugri tenging við LUKR?
  - Sjá verkefnin á korti
- Gera talningu atkvæða sýnilegri?

Lokaorð

- Mikilvægt og lærdómsríkt verkefni
- Unnið af miklu kappi og áhuga
- Stundum tekist á um leiðir
- Þakka árangursríkt samstarf