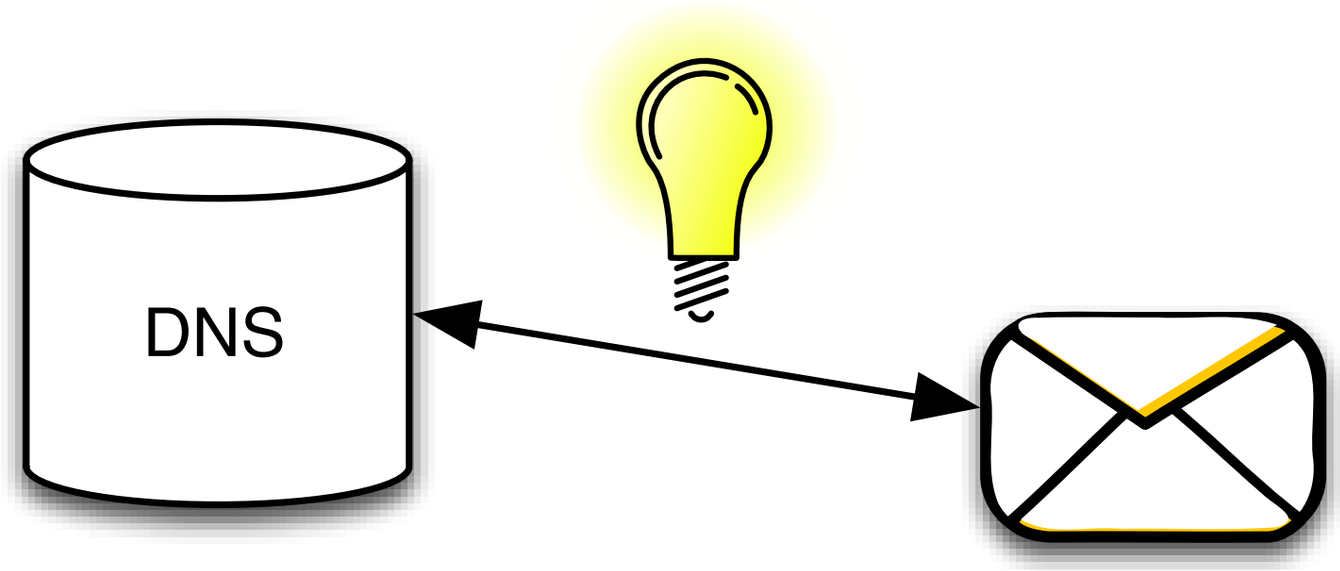
DKIM

Domain Keys Identified Mail

kirei

Vad gör DKIM?



kirei

DomainKeys

kirei

DKIM

kirei

Okänsligt för väg

bygger på elektroniska signaturer

kirei

Verifiering
underlag till klassificering

kirei

Giltig signatur?
Trovärdig signatur?

kirei

Påbyggnad

retrofit

kirei

Funktionella krav

kirei

Funktionella krav

kirei

Funktionella krav

✓ tillhandahålla identifiering på domännivå

kirei

Funktionella krav

- ✓ tillhandahålla identifiering på domännivå
- ✓ kunna delegera ansvaret för signering till tjänsteleverantörer

kirei

Funktionella krav

- ✓ tillhandahålla identifiering på domännivå
- ✓ kunna delegera ansvaret för signering till tjänsteleverantörer
- ✓ identifiering och hanteringspolicy är två skilda saker

kirei

Funktionella krav

- ✓ tillhandahålla identifiering på domännivå
- ✓ kunna delegera ansvaret för signering till tjänsteleverantörer
- ✓ identifiering och hanteringspolicy är två skilda saker
- ✓ bibehålla möjligheten till anonyma meddelanden

kirei

Operationella krav

kirei

Operationella krav

- ✓ signaturer skall vara transperenta för system som inte implementerar funktionaliteten

kirei

Operationella krav

- ✓ signaturer skall vara transperenta för system som inte implementerar funktionaliteten
- ✓ en felaktig eller ogiltig signatur är jämställd med ingen signatur alls

kirei

Operationella krav

- ✓ signaturer skall vara transperenta för system som inte implementerar funktionaliteten
- ✓ en felaktig eller ogiltig signatur är jämställd med ingen signatur alls
- ✓ kunna införas gradvis, med gradvis förbättring av nyttan

kirei

Operationella krav

- ✓ signaturer skall vara transperenta för system som inte implementerar funktionaliteten
- ✓ en felaktig eller ogiltig signatur är jämställd med ingen signatur alls
- ✓ kunna införas gradvis, med gradvis förbättring av nyttan
- ✓ minimera krav på omgärdande infrastruktur

kirei

Sker under huven

kirei

Filtrering baserat på signaturer?

kirei

Signerande parts trovärdighet räknas!

kirei

SSP

Sender Signing Practices

kirei

Signeringspolicy

DKIM-SSP

kirei

Publicering genom DNS

```
_ssp._domainkey.kirei.se.    IN    TXT    "dkim=all\; t=s"
```

kirei

Överensstämmelse

From-fältet [RFC2822]
Signerande parts identitet

kirei

Giltig signatur?

kirei

Rekommendation

- kasta
- betrakta som suspekt
- allt är i sin ordning

kirei

Blockera

_ssp._domainkey.kirei.se. IN TXT "dkim=strict\; handling=deny"

kirei

Tekniken

kirei

Nyckelhantering

kirei

Selektor

```
[selektor]._domainkey.example.com

nov2007._domainkey.kirei.se    IN    TXT   “v=DKIM1\; p=MIGfM0G...
```

kirei

Nyckelbyte

```
jun2007._domainkey.kirei.se. 60 IN TXT "v=DKIM1\; p=MIGfMA0GCSqGSIb..
nov2007._domainkey.kirei.se. 60 IN TXT "v=DKIM1\; p=MIGfMA0GCSqGSIb..
```

kirei

Delegering

```
nyhetsbrev11._domainkey.kirei.se.   IN CNAME dkim.reklamfirman.se.

dkim.reklamfirman.se.               IN TXT "v=DKIM1\; p=MIGfMA0GC..
```

kirei

Signerande part

Vad krävs?

kirei

Potentiella fallgropar

signering

kirei

Verifierande part

Vad göra?

kirei

Potentiella fallgropar

verifierande part

kirei

Nytta idag!

kirei

Klientstöd?

kirei

Säkerhetsaspekter

kirei

Sårbarheter

Utnyttjande av längdangivelse

kirei

Sårbarheter

röjande av privat nyckelmaterial

kirei

Sårbarheter

DNS

kirei

Sårbarheter

Informationsläckage

kirei

Sårbarheter

Insider

kirei

Sårbarheter

Missbruk av domän

kirei

VBR

Vouch By Reference

kirei

Trovärdig avsändare?

kirei

Oberoende tredje part

VBR-Info: md=kirei.se; mc=transaction;
mv=tredjepart.se:schyssta.org;

kirei

Litar jag på ..?

kirei

VBR i DNS

kirei.se._vouch.tredjepart.se IN TXT "transaction list"

kirei

VBR i intressegrupper?

kirei

Vitlistor!?

kirei

Summering

kirei

DKIM
DKIM-SSP
DKIM-SSP + VBR

kirei

Referenser

http://dkimproxy.sourceforge.net/
http://dkim.org/info/dkim-faq.html
http://dkim.org/

http://www.ietf.org/rfc/rfc4871.txt

http://www.domain-assurance.org

kirei

Sårbarheter

Missbruk av domän

kirei

fredrik@kirei.se

kirei