DNSSEC och säkerheten på Internet

Per Darnell

2000-10-16
1

Säkerheten på Internet

- Identitet
- Integritet
- Oavvislighet
- Alltså…

2000-10-16
2

Asymmetrisk nyckelkryptering

Bengt

2000-10-16
3

Asymmetrisk nyckelkryptering

1 Utbyte av publika nycklar

Bengt

Asymmetrisk nyckelkryptering

1 Utbyte av publika nycklar

2 Bengt skapar en transaktion

3 Bengt skapar en hashkod, en checksumma över transaktionen

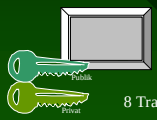
4 Hashkoden signeras med Bengts privata nyckel

5 Den signerade koden adderas till transaktionen

6 Transaktionen krypteras med en engångsnyckel

7 Engångsnyckeln krypteras med bankens publika nyckel

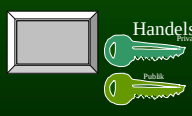
8 Transaktionen skickas



Bengt

Asymmetrisk nyckelkryptering

1 Paketet öppnas och den symmetriska engångsnyckeln dekrypteras med bankens privata nyckel



Bengt

Asymmetrisk nyckelkryptering

1 Paketet öppnas och den symmetriska engångsnyckeln dekrypteras med bankens privata nyckel

2 Transaktionen dekrypteras

3 Hashkoden verifieras med Bengts publika nyckel

4 Genom rehash kan man i efterhand kontrollera att transaktionen inte ändrats sedan Bengt en gång signerade den med sin privata nyckel

Bengt

PKI vs DNSSEC

PKI

- Asymmetrisk nyckelkryptering
- Löser identiteten mellan två parter
  - Ex webbplats och surfare
- Ger oavvislighet
- Skyddar information

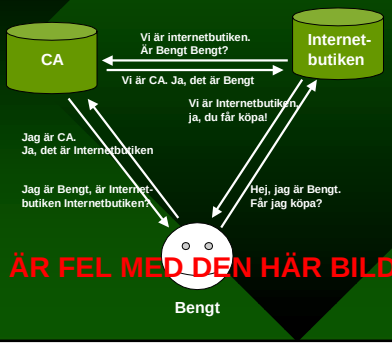
DNSSEC

- Asymmetrisk nyckelkryptering
- Löser identiteten mellan DNS-servrar

Vem är passmyndigheten på Internet?

- Publik CA (Certificate Authority)
  - I Finland har man infört ett nationellt system för digitala ID (EID). Sverige har Posten och Telia
  - Fördel: infrastrukturen finns
  - Nackdel: användarna saknas
- Banken
  - Har hundratusentals användare
  - Intressanta samarbeten pågår

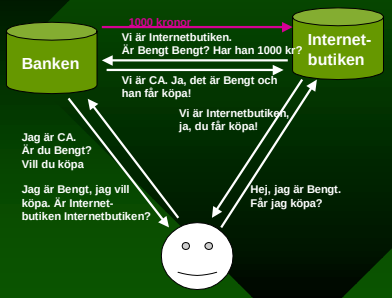
CA-modellen



VAD ÄR FEL MED DEN HÄR BILDEN?

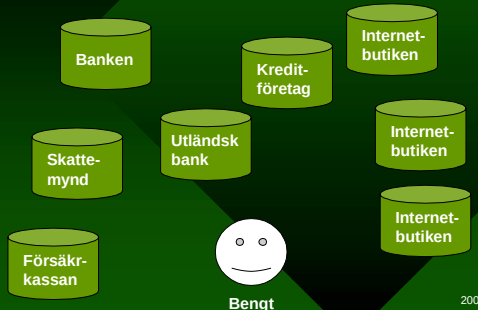
2000-10-16
10

Bank som CA



2000-10-16
11

Vilka vågar lita på banken?



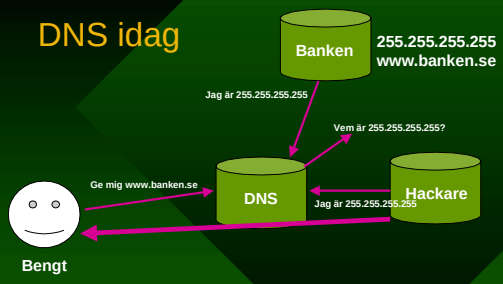
2000-10-16
12

DNS roll i Internet

- DNS översätter namn som www.banken.se till ett ip-nummer: 199.234.23.17
- Idag finns ingen säkerhet i DNS. En tonåring med NT kan enkelt låtsas vara bank på Internet
- Det enda som gör att du kan veta att du är på banken är att hänglåset i din webbläsare är låst
- En webbsajt kan aldrig veta vem som surfar om de inte använder digitala certifikat.

2000-10-16
13

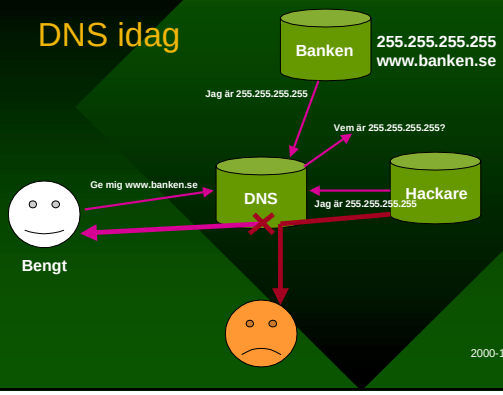
DNS idag



Den som svarar först är 255.255.255.255, dvs www.banken.se

2000-10-16
14

DNS idag



2000-10-16
15

DNS som CA för Servrar:

- DNSSEC Kommer i BIND 9
- Endast de servrar som är legitima vidarebefordras till surfarna – dvs godkänns
- Användarna vet att de hamnar hos rätt webbplats

DNS som CA för användare?

- Alla förbindelser blir säkra
- Användarna inte längre anonyma
- Webbplatserna kan mycket enkelt samla mängder av information om användarna
  - Surfvanor, vilka webbplatser de besökt, vilka sidor de tittat på etc.
- Kommer användarna att vilja använda certifikat
- Kommer webbplatserna vilja använda certifikat?

Säkerhet idag

- Focus på möjlighet att kunna ha en identitet för elektroniska affärer
- Snart kommer fokus att skifta till personlig integritet
- NIC-SE:s roll är att se till att Internet fungerar i Sverige oavsett vad debatten handlar om.