Digitale Handtekening
Praktische problemen bij toepassingen

TestNet: Testen van Security

ING Group, April 2006
Ruud Goudriaan

ING

Digitale handtekeningen

- Korte uitleg Asymmetrische Cryptografie
- Hoe gebruik je digitale Handtekeningen
- Welke praktische problemen kun je verwachten
- Wat moet je testen

ING

Symmetrische Cryptografie

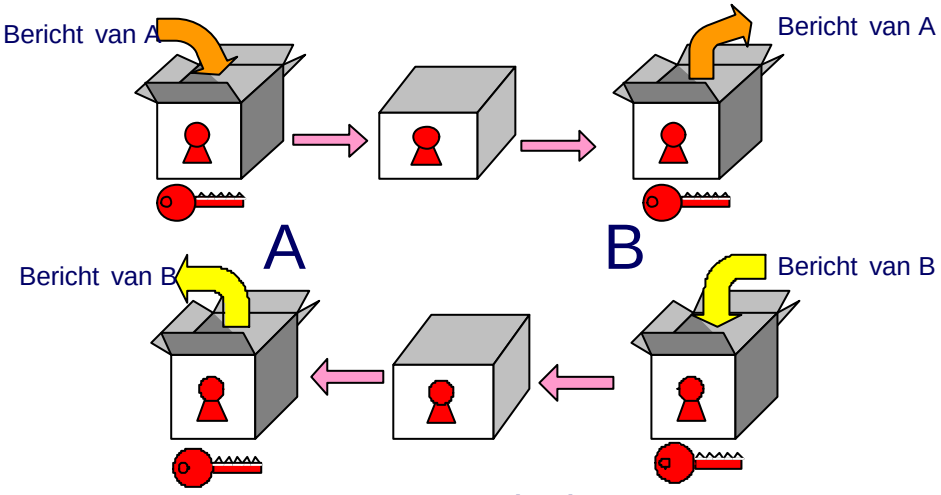
Symmetrisch

DES

ING

3

Beide partijen zelfde geheime sleutel



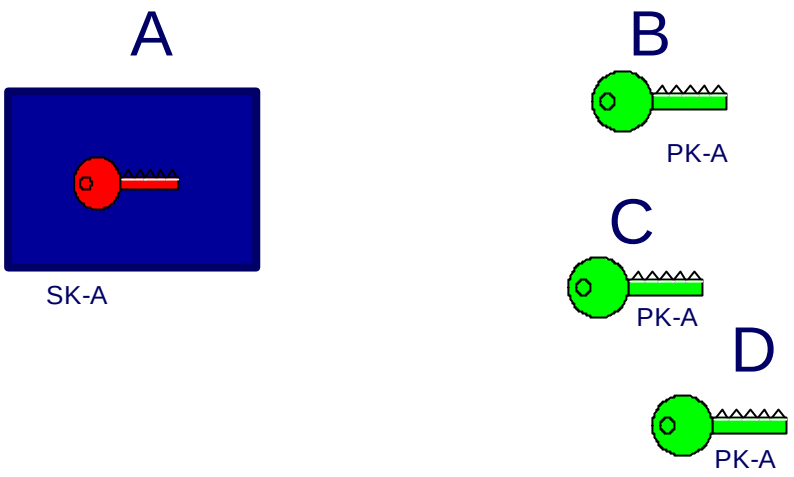
Symmetrisch

DES

ING

4

Asymmetrische: Public en Secret key



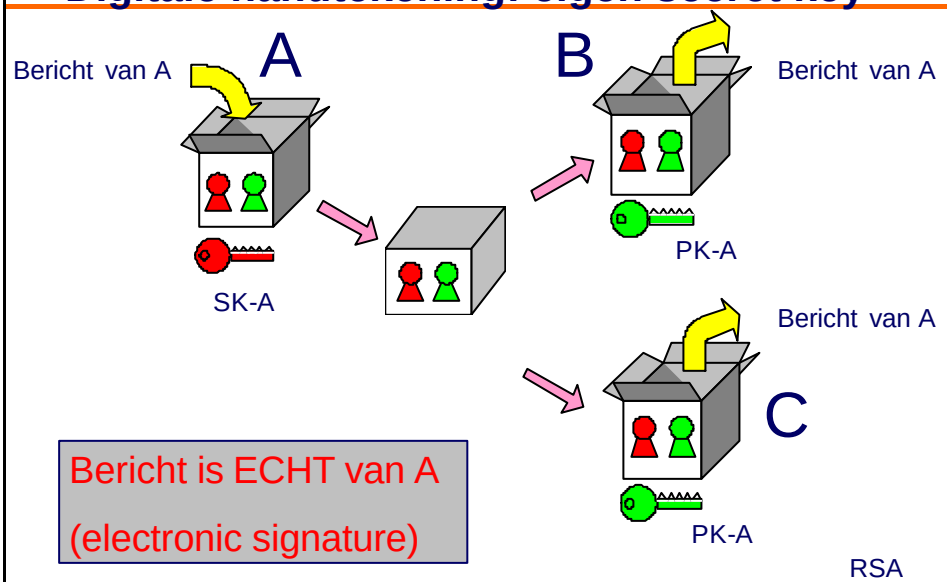
Asymmetrisch

RSA

5

ING

Digitale handtekening: eigen secret key



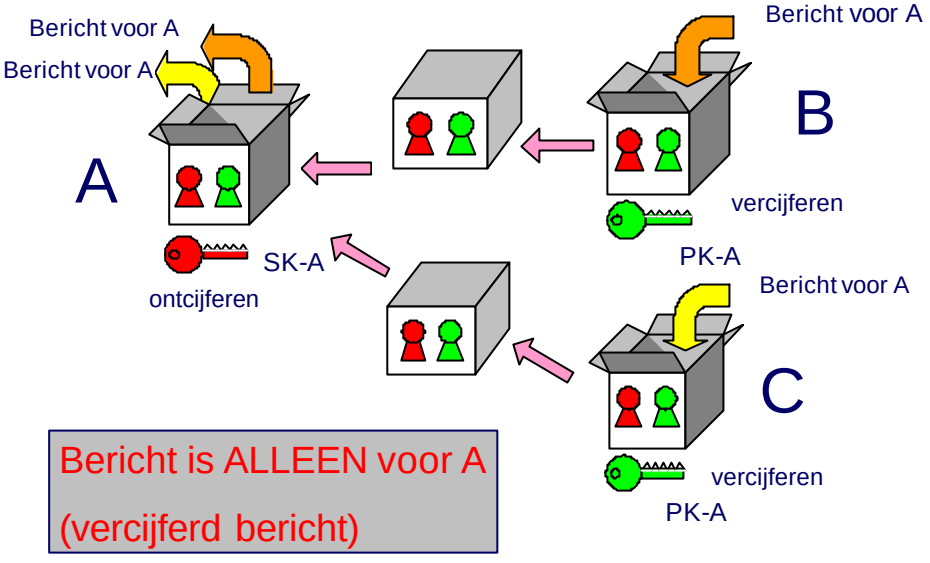
Bericht is ECHT van A
(electronic signature)

RSA

6

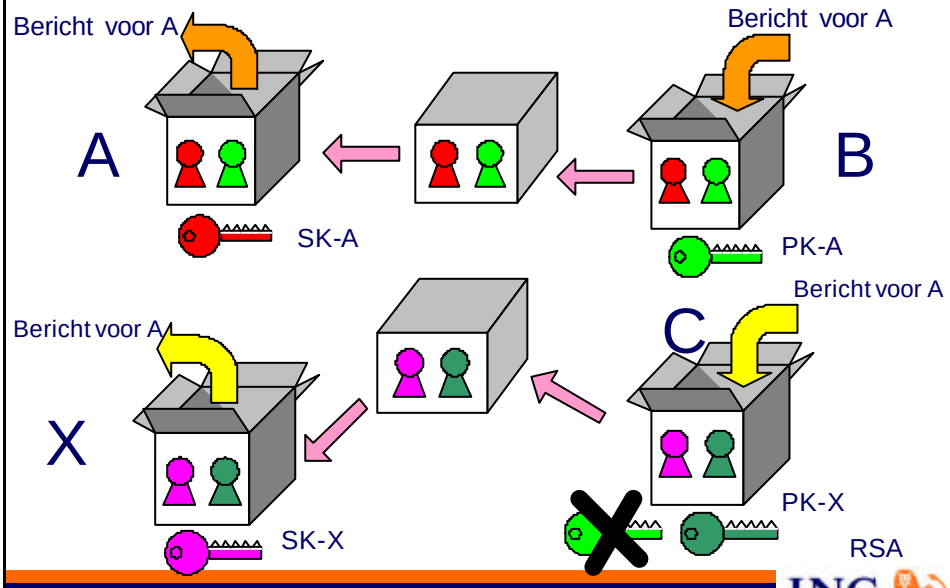
ING

Vercijfering: public key ontvanger



7

Aanval: X vervangt PK-A voor PK-X



8

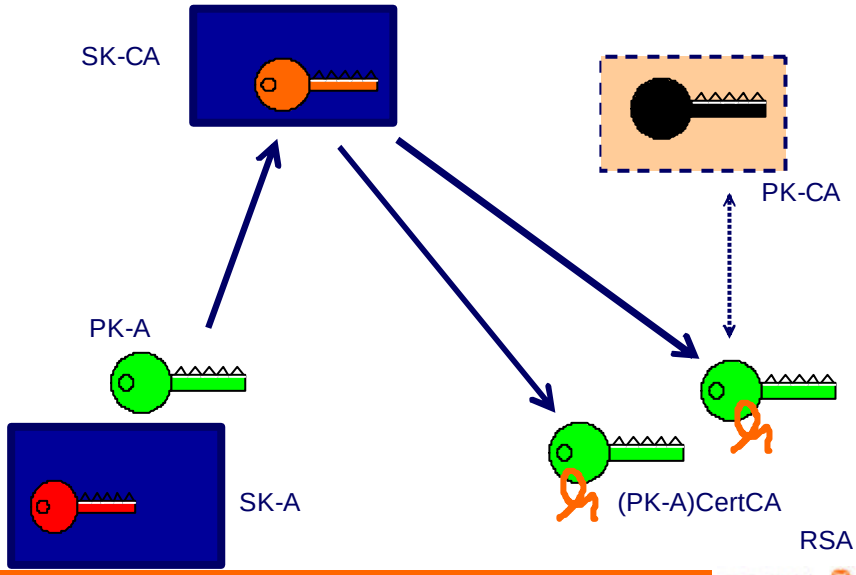
Oplossing: Certificaat Public key

- Openbaar ‘Telefoonboek’
- Browser software
- Certification authority

9

ING

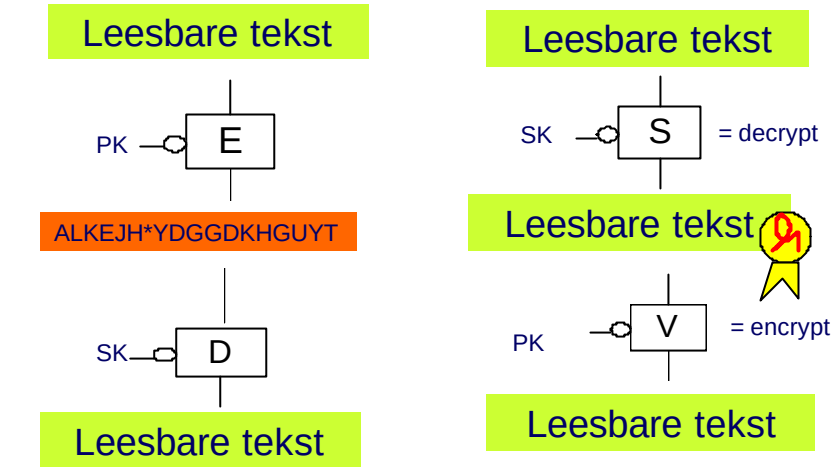
Certification Authority ‘signed’ PK-A



10

ING

Schematisch weergave ‘sign’ en ‘encrypt’



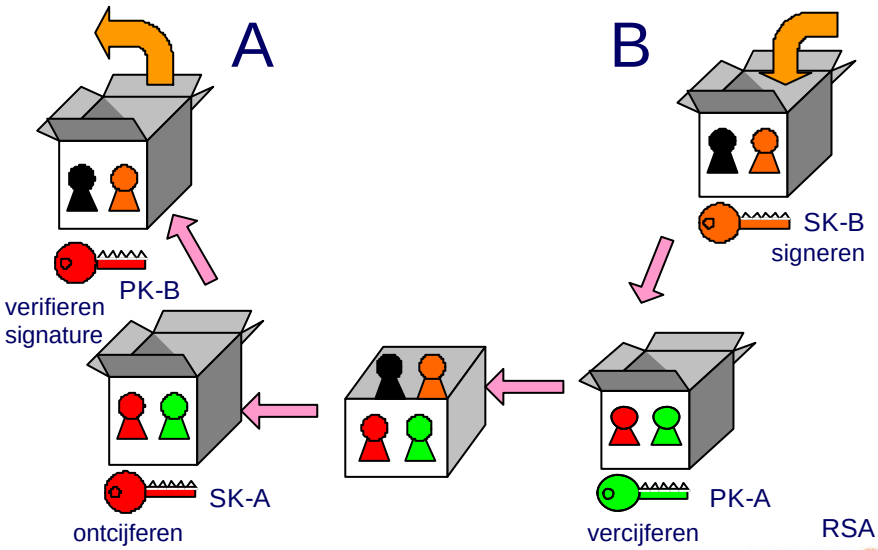
Encrypt = Vertrouwelijkheid

‘Sign’ = Authenticiteit

11

ING

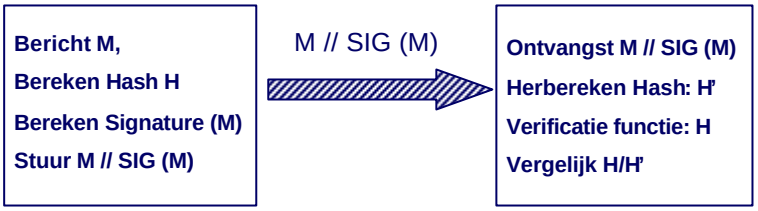
Signing en Encrypting: end-to-end secure



12

ING

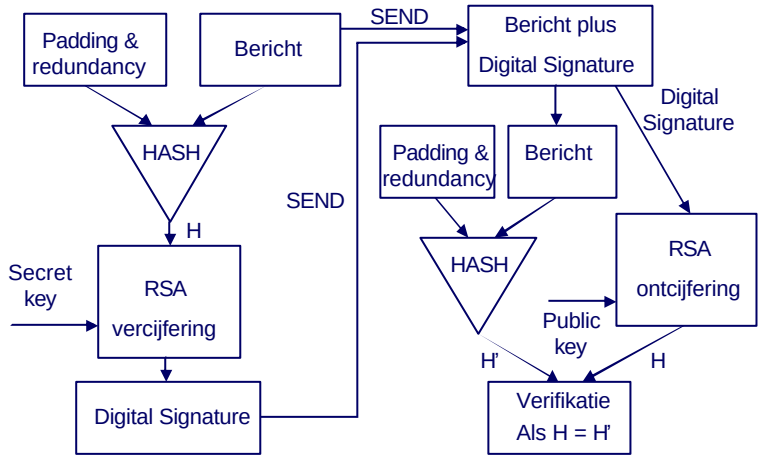
Bericht autorisatie: Digital Signature



Digital Signature: mechanisme voor bericht autorisatie
Essentieel: bijbehorende Hash-functie van gelijke sterkte.
Goede Hash funktie: SHA-160, voorbereiden op SHA-256

ING

RSA blokschema: Text hashing mode



Text hashing mode of signature

ING

Secure Mail: encrypted mails/attachments

SECURE MAIL
ING employees that exchange confidential documents with external, but trusted, parties should get 'Secure mail' to send and receive encrypted e-mails and attachments.

Secure mail means an addition to the desktop in the office in the form of a **Reader, Chipcard and USB-cable**.

Chipcard contains CERTIFICATE of Public Key

ING

Establish Secure Mail relationship

Three possibilities:

1. **End-to-end relationship (workstation-to-workstation)**
2. **Mailgateway-to-Mailgateway relationship**
3. **End-to-Mailgateway relationship**

Bij 2. Centraal punt encrypt/decrypt en distribueert namens de eindgebruikers

Bij 1. Alleen eindgebruiker kan bericht ontcijferen of digitale handtekening zetten

Bij 1. Worden bilateraal certificaten uitgewisseld

Bij 2. Worden Mailgateway certificaten uitgewisseld

Bij 3. Moet de Mailgateway eindgebruikers simuleren

ING

Initial exchange of certificates

1. Partijen sturen elkaar ‘Signed’ mail: ING e-mail bevat door ING Root getekend certificaat (=PK-ING); Externe e-mail bevat door CA externe ondertekend certificaat (=PK-Externe). Partijen slaan elkaars Certificaten op en geven het kwalificatie: Certificaat expliciet wel vertrouwen (Cross-Certification)
2. Mail gateways wisselen ‘company-certificates’ uit en encrypten/decrypten alle berichten met dezelfde keys
3. Mail gateway slaat certificaat bericht eindgebruiker op en gebruikt dat bij encryptie antwoordbericht

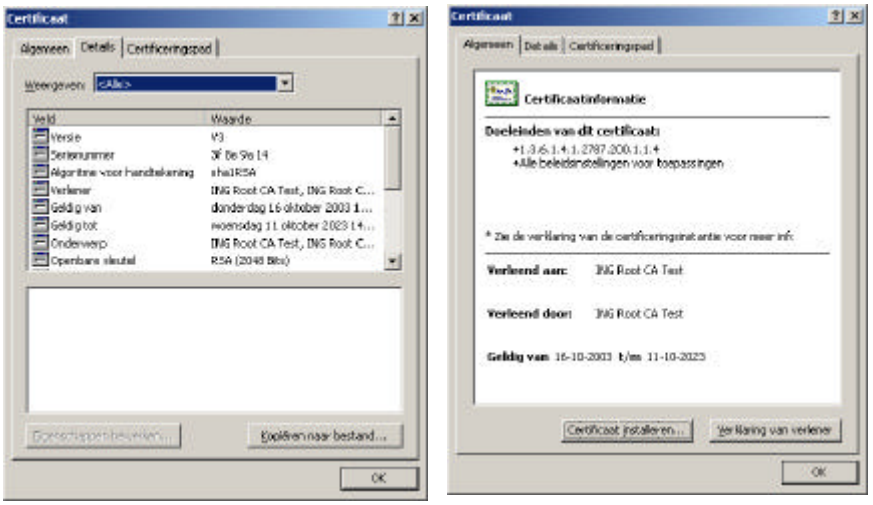
ING

Testen voor Secure mail

- Klopt protocol Certificaat
- Is certificaat te vertrouwen (trusted CA)
- Is certificaat van voldoende kwaliteit (encryptie)
- Accepteert Mail gateway of Eindgebruiker certificaat
- Is certificaat opgeslagen in Lijst Contactpersonen (of in Global Address List)
- Is Chipkaart geldig en juist geactiveerd

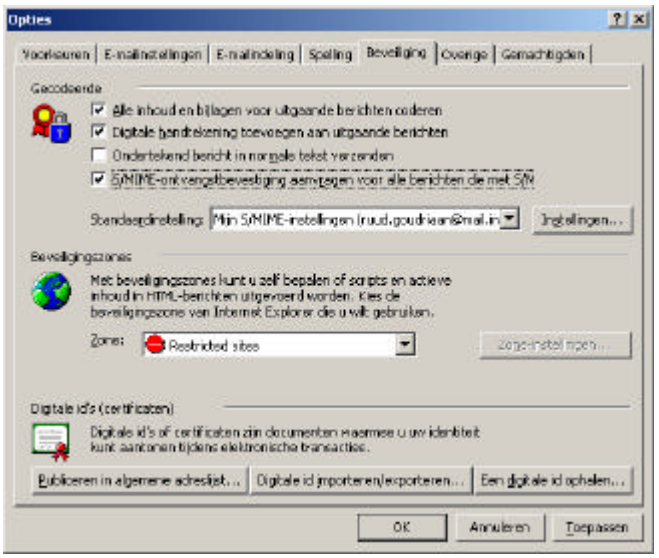
ING

Certificaatschermen



ING

Beveiligingsinstelling Outlook



ING

Wat kan er mis gaan?

A. Verzonden bericht anders dan Ontvangen bericht waardoor Signature niet klopt
B. Aangeboden certificaat eindgebruiker bevat optionele velden die door Mailgateway niet worden geaccepteerd
C. Externe eindgebruiker heeft geen of niet compatibel Digitaal handtekening systeem
D. Eindgebruiker kan ontvangen encrypte berichten niet lezen of openen
E. Eindgebruiker krijgt waarschuwing dat Digitale handtekening ontvangen bericht niet betrouwbaar is
F. Eindgebruiker stuurt ontvangen beveiligd bericht per ongeluk zonder beveiliging door

ING

Vragen?

Mail eventuele vragen door naar:

ruud.goudriaan@mail.ing.nl

ING