Certificates --
How many do we really need

Taher Elgamal

Netscape Communications

NETSCAPE

Certificates --

What are they

- Signed message by a trusted third party that binds of a public key with its “owner”
- Used to prove that a person or an entity owns a public key and optionally has some other characteristics
- The trust in the binding depends on the trust in the policies and procedures used by the third party
- A collection of certificates is analogous to an “electronic wallet”

NETSCAPE

Certificates --
why different ones

- Certificates are used for different purposes
- Different certificates need different “trust levels”
- Validity period of a certificate depends on its use
- Prevent a credit card from being used as an ID
- Established relationships may result in very specific certificates that have no particular meaning outside

NETSCAPE

Identity-type certificates

- "Drivers license" equivalent in the electronic world
- Issuing an ID card implies a check of the identity of the card holder
- Used by servers to identify their ability to conduct business electronically using a particular business name
- Used by corporations to identify employees, consultants, vendors, customers and so on.

NETSCAPE

Authorization-type certificates

- Embedding authorization rights for document retrieval into certificates
- May be used by corporations to identify access capabilities of an employee or affiliate
- May be used by banks to identify certain “class” of customers

NETSCAPE

Special purpose certificates

- Financial certificates for account based payments
- Bank certificates for communicating privately with a customer
- “Entity” certificates, for example a Human Resource certificate
- Machine certificates, for example a certificate identifying a DNS or a mail server

NETSCAPE

So, how many certificates do I really need

- A universal certificate is possible to design but quite complicated
- Different countries have different styles when it comes to “how many cards do you have in your wallet”
- Likely outcome is to have a similar number of certificates as the number of cards in your wallet

NETSCAPE