

PGP for commerce, why not?

OpenFortress*
digital signatures

which technologies are popular?

- * PGP in the hacker community

- * X.509 in commercial circles

- * XML Signing, anyone?

- * Why this difference?

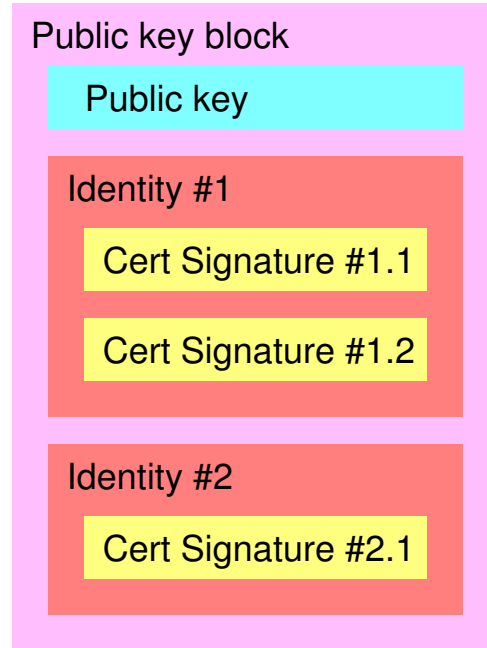
- * Is PGP too difficult?

- * X.509 makes sense for LDAP

inside out certificate structures



X.509:
strict hierarchy



PGP:
multiple signers

top down or bottom up trust



X.509:
Islands of trust separate



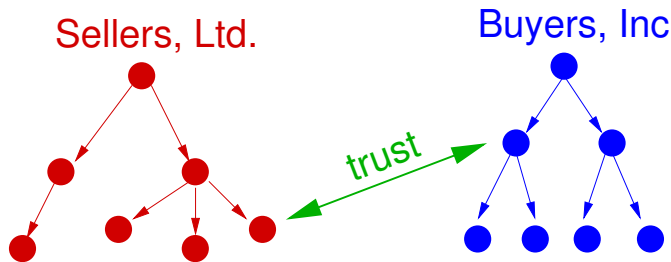
PGP:
Islands of trust integrate

lock in by certificate signer

- * X.509 certificates point to one signer
- * This continues until a root cert
- * Effectively a lock-in by the certificate signer
- * Certificate signers boost signing technology
- * So... commercial focus on X.509

commercial trust is peer to peer

- * Companies know each other directly: peer-to-peer
- * Or through contact networks: web-of-trust
- * X.509 CA's are often overkill:



- * But lacking e.g. PGP-SASL in browsers. . .

browsers only do tls/ssl

- * Myth: Browser apps are simple
- * Reality: Browser takes full control :-)
- * Legal: Will it hold up in court with users not in control?

- * Browsers cannot hide conceptual complexity
- * Browsers should not hide conceptual complexity

formats to sign

* Myth: HTML is user-friendly

* Reality: Dynamic HTML can trick its viewers

* Legal: Will it hold up in court if DHTML is signed?

* Myth: XML makes everything compatible

* Reality: XML has no semantics

* Legal: Will it hold up in court if semantics are assumed?

formats to sign

Every end user *must* understand document source. . .

* . . .so HTML is *not done*

* . . .and XML is *not done*

* . . .but ASCII is *well done!*

least troublesome signatures

- * Plain text
- * User in control
- * Simple peer key registration

Sounds like...

- * PGP as signing technology
- * Mail as signing application

do we need identity?

Technically, only keys matter, but. . .

- * companies know each other by name
- * companies are registered by name
- * companies have a reputation by name

. . . to companies, identity matters

building trust in identities

Can X.509's PKI establish trust in an identity?

- * Yes: One policy under one root certificate
- * Yes: Central party takes responsibility
- * Yes: No intermediates involved
- * No: Disclaimers invalidate the issues above

building trust in identities

Can PGP's WoT establish trust in an identity?

- * No: OpenPGP is too fuzzy
- * No: Nobody takes responsibility
- * No: Intermediates are out of reach

Fundamental Question:

*** What is the meaning of a signature?**

we need signing policies

Signing policies are signer assertions

Technically possible and available:

- * X.509 has such an attribute built-in
- * PGP has such an attribute built-in
- * XML Signing can incorporate Reference URIs

But signing policies are rarely used. . .

- * . . . not standardised
- * . . . not automatically processable

we need signing policies

- * Instead of a URL, use a Policy URN

URN is a scheme of unique names under a named scope.

URNs fall under URIs which rapidly replace URLs in standards.

- * Works for PGP, X.509, XML Signing

- * Be certain *in spite of* OpenPGP

`urn:signpolicy:idchecked+twopaths`

- * Verification algebra looks a lot like subsetting:

`idchecked` \subseteq `idchecked+twopaths`

- * Note: Interpretation is not enforceable in S/MIME

rough policy urn syntax

urn ::= "urn:signpolicy:" polset

polset ::= polmod
| polmod "+" polset

polmod ::= polname
| polname "(" params ")"

polname ::= identifier
| hashname "=" hexstring
| "x-" identifier

standardise policy modules

- * Register urn:signpolicy through IETF
- * Have IANA register policy modules (idchecked)
- * Policy modules must meet global consensus

Note the immense difference between:

- * urn: signpolicy:idchecked
- * urn:x-signpolicy:idchecked

what openfortress is doing

People involved:

- * Rick van Rein
- * Edwin Woudt

Actions and plans:

- * Building policy verifier (GPL library)
- * Building example application
- * Hoping to standardise in an RFC...

Currently: Looking for feedback!

applications of signing policies

- * Strong statements about identity
- * Transitive closures for the Web of Trust
- * PGP key with *same owner* (no trust hop)
- * *I read and understood* what I sign
- * *Willing to pay* for signed job
- * ...
- * Brainstorming...

questions and remarks?

Shout now...

...or mail us later.

`signpolicy@openfortress.nl`

`http://openfortress.nl/news/projects/signpolicy/`

Thanks!

info@openfortress.nl

http://openfortress.nl

OpenFortress*
digital signatures