PGP/GPG vs. PKI

Laura Raderman

GEMINI
SECURITY SOLUTIONS

Who am I?

- Director of Security Assessments - Gemini Security Solutions
- Participated in the Federal PKI working group
- Provide consulting services for large enterprise PKIs
- Occasionally Pen-testing
- CMU MS in Information Networking

GEMINI SECURITY SOLUTIONS

Outline

- Public Key Cryptography
- PGP/GPG
  - Key Management
  - Trust issues
- PKI
  - Key Management
  - Trust issues
- Why choose one over the other?

GEMINI SECURITY SOLUTIONS

Public Key Cryptography

- Two keys – public and private
- Mathematically related (trapdoor functions with high computational complexity)
  - If you know the public key, it's very computationally complex to get the private key – unless you have the "key" to the trapdoor
- Several algorithms:
  - RSA (computing factors)
  - DSA and ElGamal (computing logarithms)

GEMINI SECURITY SOLUTIONS

Public Key Cryptography

- The basic premise is that each key “un does” what the other did.
  - Your private key decrypts what was encrypted with your public key
- More (very mathematical) information:
  - Handbook of Applied Cryptography (Chapter 8) http://www.cacr.math.uwaterloo.ca/hac/
  - Practical Cryptography – Neils Ferguson and Bruce Schneier

GEMINI SECURITY SOLUTIONS

Public Key Cryptography

- Allows for more than just encryption/decryption
  - Digital Signatures
  - Message Integrity
  - Key Exchange and Agreement
- … And, all of this without having to exchange keys in an out of band manner

GEMINI SECURITY SOLUTIONS

Digital Signatures

- Using a private key to encrypt something is called signing
- Usually you only encrypt a hash of the data you are "signing"
- Provides:
  - Non-repudiation (denying you sent it) – **private** key
  - Message Integrity – uses the public key to decrypt the hash. If the hashes match, the message has not been altered

GEMINI
SECURITY SOLUTIONS

So, how **do** we share public keys?

- Give them to your friends
- Publish them on your web site
- Keyservers
- X.500/LDAP directories

- They are public after all, you don't have to worry about who has your public key

GEMINI
SECURITY SOLUTIONS

BUT

- What about all of the public keys you've collected (that aren't yours)?
- How do you know that the person who has the corresponding private key is who you think they are?

- Here's where PGP and PKI differ

PGP

GEMINI
SECURITY SOLUTIONS

GEMINI SECURITY SOLUTIONS

PGP

- Pretty Good Privacy
- PGP was originally created in 1991 by Phil Zimmermann and has gone through many iterations and owners since then
- Currently, PGP is owned by the PGP Corporation, which sells PGP Desktop and PGP Enterprise software
- OpenPGP was “created” as an IETF working group in 1997 in order to create an open standard for PGP (RFC 4880, RFC 3156)
- All the details here refer to OpenPGP (and GNU’s implementation of OpenPG - GPG)

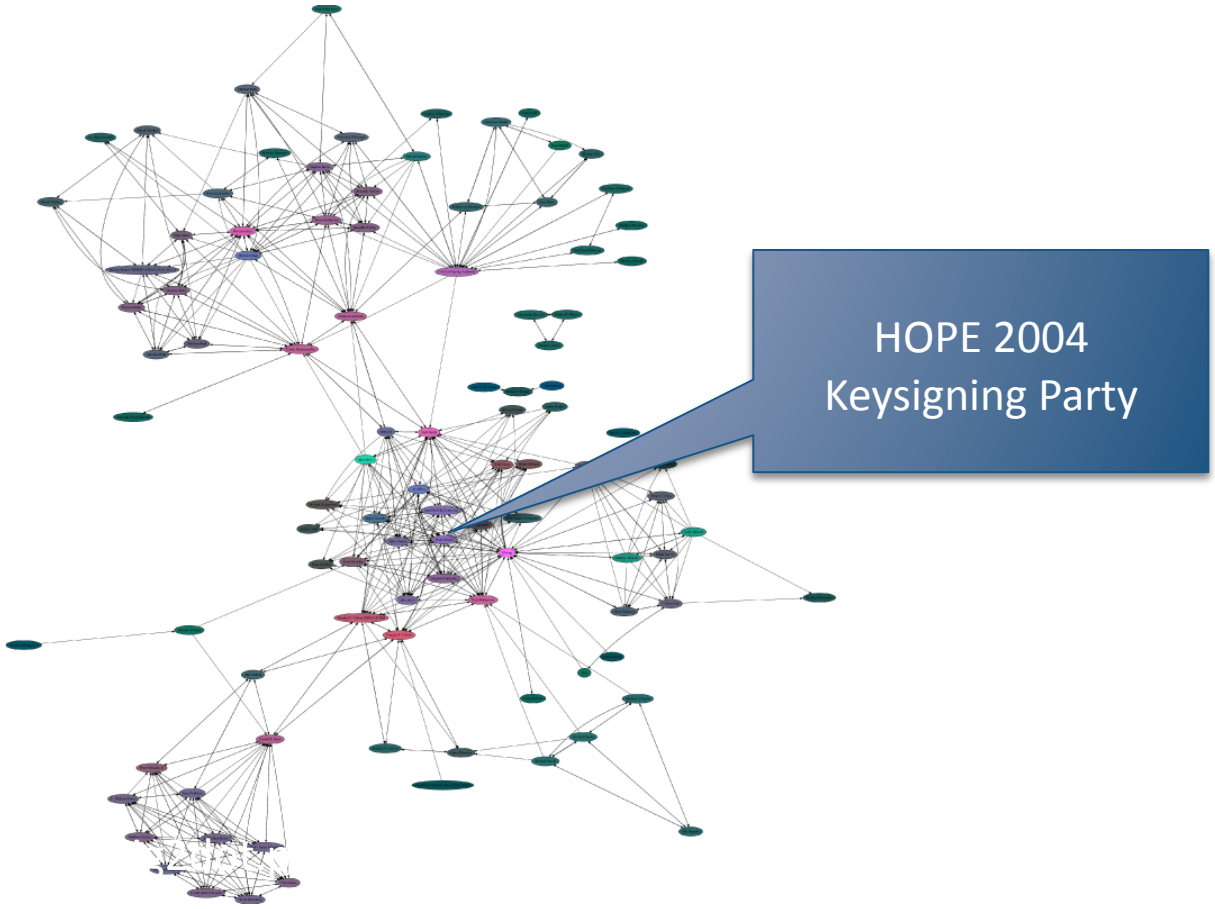
GEMINI SECURITY SOLUTIONS

OpenPGP – Key management

- OpenPGP and the PGP Corporation support both the traditional “web of trust” model and a hierarchical model.
- Keys are kept on a “key ring” (or multiple key rings). Each user will have at least two key rings, one for private keys, and one for public keys.
- Most public keys are exchanged in an ad hoc manner
  - There are PGP key servers that can be used to store and retrieve public keys
  - Users select what keyserver(s) they want to use

GEMINI
SECURITY SOLUTIONS

Web of Trust (mine)



GEMINI SECURITY SOLUTIONS

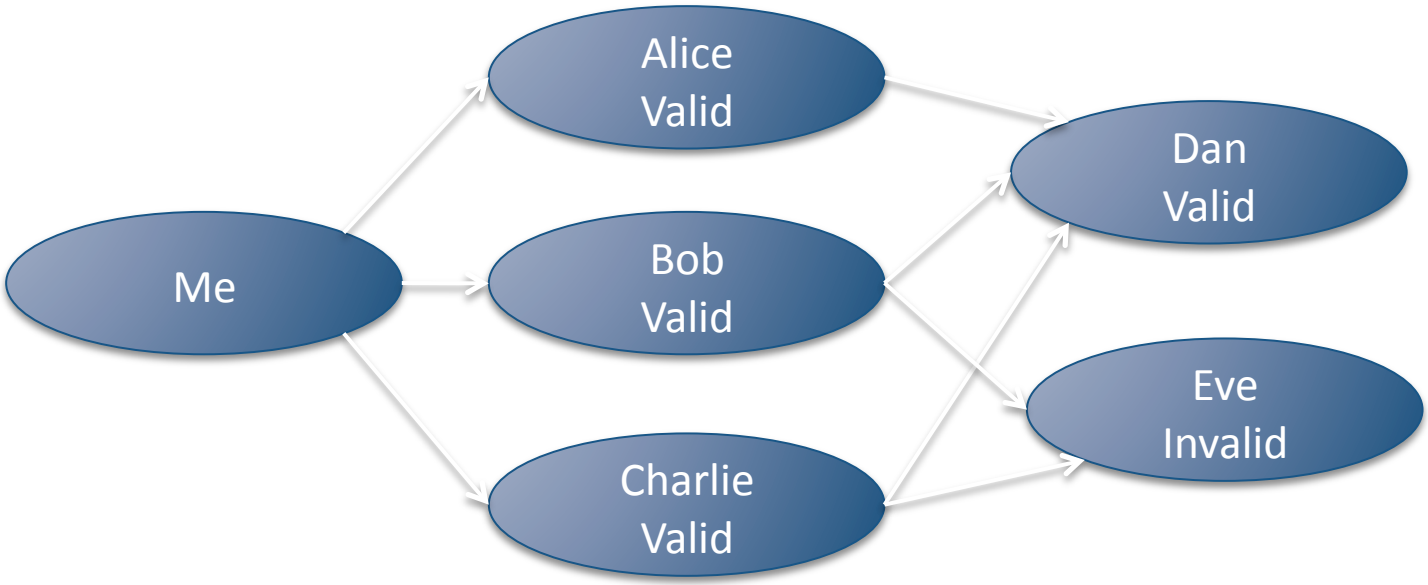
Validating a Key (for encryption/data signing)

- Four levels of trust for validating (user sets the trust level with -–update-trustdb):
  - Don’t trust
  - Don’t know
  - Marginal
  - Full
- In order to validate a key, GPG requires
  - Enough valid keys
  - The key being validated must be within 5 steps of yours (default)

GEMINI SECURITY SOLUTIONS

What's "enough" valid keys?

- GPG defaults to requiring one of:
  - A key you've personally signed
  - One fully valid key must have signed it
  - Three marginally valid keys must have signed it



GEMINI SECURITY SOLUTIONS

Where do you find the keys in the middle?

- Me -> Alice -> Bob -> Charlie
- Charlie sends me a signed e-mail, but I don't have Charlie's key in my keyring, only Alice's
- How do I find out that link between Alice and Charlie is Bob (and if Bob is fully or marginally trusted)?
  - Recursively search key servers
  - Ask Alice if she knows
  - Ask Charlie if he knows
- One of the problems with a decentralized web of trust

GEMINI SECURITY SOLUTIONS

OpenPGP – Trust Issues

- OpenPGP supports a hierarchical trust model using trust signatures
- Most users use the “web of trust” model though.
- The web of trust model does not have any central authority.
  - Each person decides how much they will trust a key or signature.
  - Each person could have different standards for identity verification.

GEMINI SECURITY SOLUTIONS

Signing Keys in OpenPGP

- There are two types of key signatures in OpenPGP
  - Signature
  - Trust Signature
- The signature is verifying that you have verified the identity of the person who's key you're signing
- Your might trust your friends to verify someone else, so if you see their signature on a key, you can know that the key belongs to the person who claims it

GEMINI SECURITY SOLUTIONS

One level “chain”

- This produces only a one level chain for signing, because you don’t know the friend of a friend, so how can you trust them?
  - Even worse: Key signing party – half of those people you may not know at all
- Doesn’t go very far
- Requires you to “leave” your group to expand your web of trust

GEMINI SECURITY SOLUTIONS

Trust Signatures

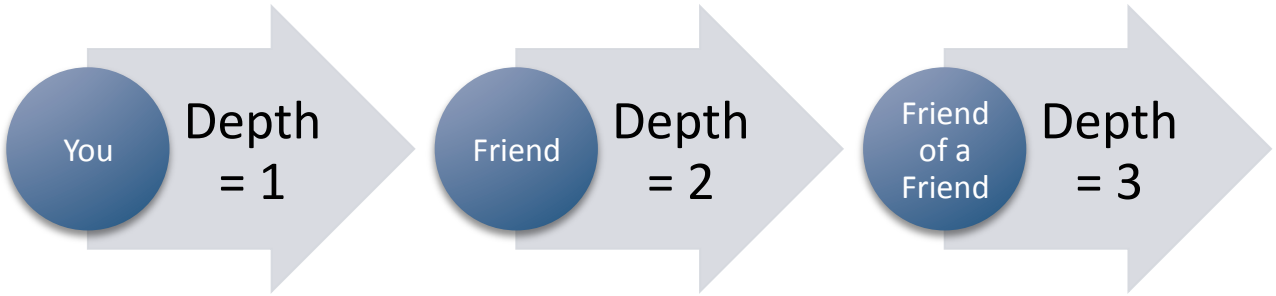
- I rarely see trust signatures
  - (gpg –-edit-key then use tsign)

```
Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I trust marginally
  2 = I trust fully

Your selection? 2

Please enter the depth of this trust signature.
A depth greater than 1 allows the key you are signing to make
trust signatures on your behalf.

Your selection? 20

Please enter a domain to restrict this signature, or enter for none.

Your selection?

Are you sure that you want to sign this key with your
key "Elwing <elwing@elwing.org>" (6680922A)
```

GEMINI SECURITY SOLUTIONS

Trust signatures

- When you make a trust signature, you're telling other people that you trust your friend to:
  - Verify a key owner's identity
  - Make trust signatures on your behalf (if depth > 1)
- You've just become a Certification Authority (of sorts)
- The depth tells others how far you trust your friend's friends
  - Depth is a measure of "chain" length



GEMINI SECURITY SOLUTIONS

PGP - Revocation

- First, you have to generate it
  - Not many people generate the revocation information when they create the key as advised in the GnuPG guide
  - When you've lost the key, how do you generate the revocation information?
- You and only you can revoke your certificate
- You **can** generate a revocation for a certificate (unless you used nrsign)

GEMINI SECURITY SOLUTIONS

Revocation (cont)

- Publish revocation information
  - Supposed to publish to all locations you previously published your public key
  - But if you published it on a web site, how do you know who has it?
- How do you notify people that you've revoked your key?
  - How do you know everyone who signed your key if they didn't upload to the same keyserver(s) you use?

GEMINI
SECURITY SOLUTIONS

So what's the problem?

- Lack of standards for identity verification.
- How do you know what verification a friend of a friend is doing?
- Referred trust is shaky, and even most trust signatures I do see only have a depth of 1 or 2
- The paranoid person is likely to *never* use a trust signature
- This is a very flexible model, allowing each person control
- Still have the problem of finding the keys in the middle
- Revocation Notification

PKI

GEMINI
SECURITY SOLUTIONS

GEMINI
SECURITY SOLUTIONS

PKI

- Public Key Infrastructure
- RFC 5280 (supersedes RFC3280)
- X.509
- Certificates
- Hardware tokens
- Policies
- Directories

GEMINI SECURITY SOLUTIONS

PKI – Basics

- Primarily a hierarchical model, but can support a web of trust like model (has interoperability challenges)
- Certificates are public keys that have been signed by another entity
- Certification Authorities issue certificates (to both other Certification Authorities and users
- Root CA – an entity with a self signed certificate
  - This is the CA that a user will trust

GEMINI SECURITY SOLUTIONS

PKI - Basics

- Subordinate CA
  - A Certification Authority without a self-signed certificate
  - Or where the self-signed certificate does not enter the validation path
- Validation Path
  - A chain of all certificates from the one you're validating to a Root CA that you trust
- Revocation List (CRL)
  - A list of all certificates that a particular CA has revoked

GEMINI SECURITY SOLUTIONS

Interesting parts of an X.509 certificate

- Required parts (not a complete list)
  - Subject (and subject key) – identifying information
  - Issuer (and issuer key) – Identifier of who issued the certificate
  - Validity Period
  - CRL Distribution Point – where to find the revocation list
- Optional parts
  - Key Usage – what the certificate can be used for
    - (Data) Signing
    - Encrypting
    - Code signing
    - Certificate Signing

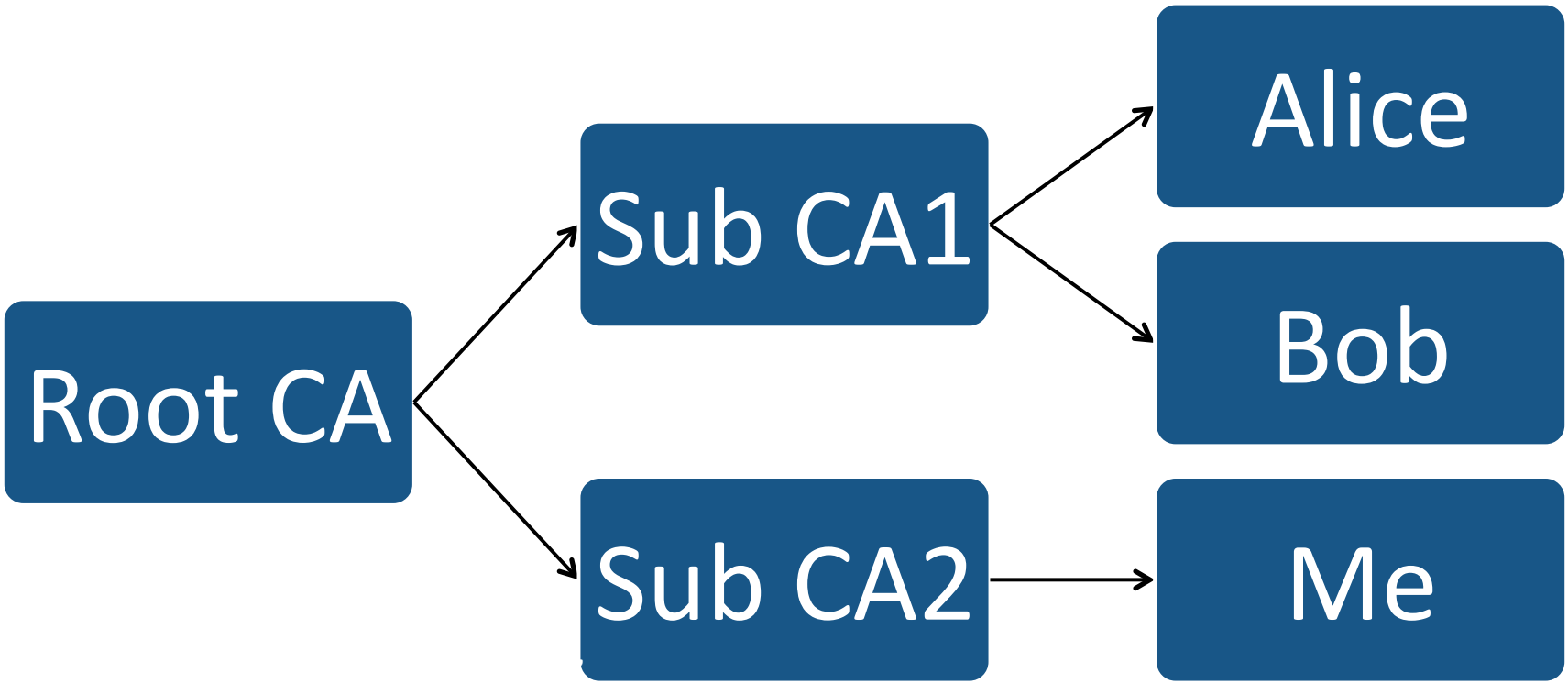
GEMINI SECURITY SOLUTIONS

Optional (cont)

- Certificate Policy
  - A link to find the certificate policy of the CA that issued this certificate
- Authority Information Access (AIA)
  - Tells the “reader” where to get the issuer’s certificate

GEMINI
SECURITY SOLUTIONS

PKI Hierarchy



GEMINI SECURITY SOLUTIONS

Path Validation

- Building a path back to a root CA you trust
- Starts with the certificate you're trying to verify
- Uses the Issuer information in each certificate, until it finds one that you trust
  - Requires the publication location of each issuer in the certificate (AIA)
- Can be more complicated than it sounds
  - RFC 4158 gives guidance on this problem

GEMINI SECURITY SOLUTIONS

PKI – Key Management

- PKI can support Key Escrow
  - The CA keeps a copy of a private key (usually encryption only)
- Great for when your employees forget their key password or lock themselves out of their hardware token
- Certificates can be published to a central directory
  - Optional, but most CA certificates are

GEMINI SECURITY SOLUTIONS

PKI - Trust Issues

- A CA should have, publish and follow a Certificate Policy (RFC 3647)
- This policy describes exactly how identity verification is done
  - What IDs are acceptable
  - How many IDs must be shown
  - Who is allowed to do the identity verification
  - How machines and devices are identified
- This is a public document, anyone can read it
- Verisign's is at: http://www.verisign.com/repository/CPS/CP_Version_2.7.pdf

GEMINI SECURITY SOLUTIONS

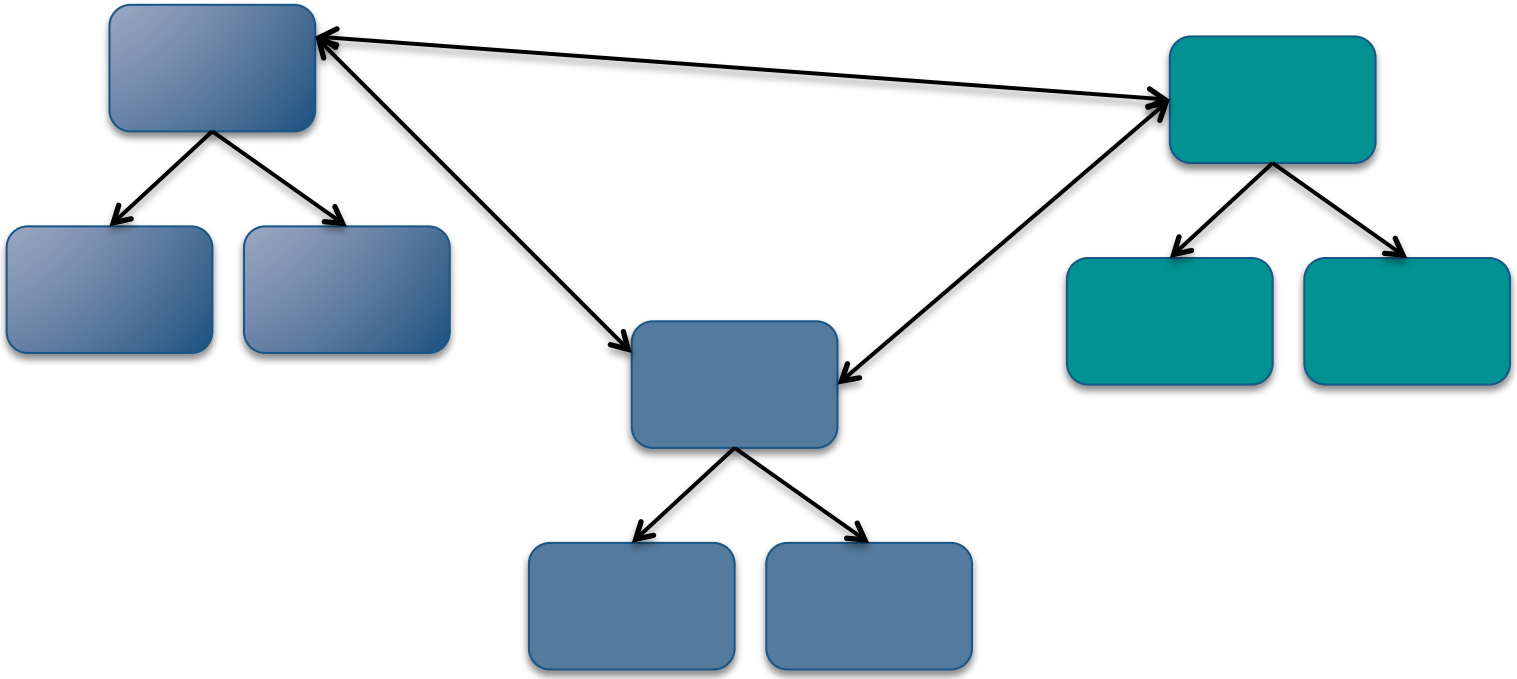
PKI – Trust Issues

- Most CAs have yearly audits
- Root CA protections
  - Offline
  - Hardware Security Module (HSM)
  - Multi-party control

- Unlike PGP where there are variable levels of trust, in PKI, the certificate is trusted, or it's not.

GEMINI
SECURITY SOLUTIONS

PKI “web mode” – Cross Certifying



GEMINI SECURITY SOLUTIONS

Cross Certificate Problems

- Policies don't always line up exactly
  - When they do, it's because a CA knew they wanted to cross-certify with a particular CA
- Politics
- Path validation becomes harder
  - Circles in the graph
- Interoperability problems

GEMINI SECURITY SOLUTIONS

Why Cross Certificates?

- Few people need to be involved
  - Everyone benefits
- Policies are mapped to each other so that they are consistent
- All end users of the PKIs can now trust the other's because the Roots trust each other
- Expands the "web of trust" for end users
  - No work on your part!

GEMINI SECURITY SOLUTIONS

PKI - Revocation

- Either the user or the CA can revoke a certificate
  - Depends on the policies
- How to find revocation information for a certificate is included in the certificate (CRL DP)
- The CA issues CRLs to the DP on a regular basis
  - CRLs can be huge (I've seen a 6MB one)
  - OCSP
- The user of the key does not control the revocation information

GEMINI SECURITY SOLUTIONS

Why choose PGP over PKI?

- Quick
- Easy to set up
- Does not require an entire infrastructure
- Best suited for informal groups, friends, and acquaintances
- Anyone can become a “CA” using trust signatures
  - Just make sure you know what you’re doing!
- Variable trust

GEMINI SECURITY SOLUTIONS

Why choose PKI over PGP?

- SSL (sorry, SSL can't use PGP – yet)
- Distribution of keys/certificates/trust information to a large number of users
- More control over subordinates
  - If they don't follow your policies, you revoke them
- Easy expansion of the "web of trust" through cross certificates
- Legal document signing

GEMINI SECURITY SOLUTIONS

Participating in PGP/GPG

- Download an OpenPGP client (http://www.gnupg.org)
- Generate your keys
- Make friends here and ask them to sign your key
  - Expect to have to show ID
- Have a keysigning party in whatever groups make sense
  - 2600 meetings
  - LUGs
- Publish your key to a key server

GEMINI SECURITY SOLUTIONS

Participating in PKI

- Public
  - CACert, Inc. (cacert.org) – Please Donate!
  - Thawte Web of Trust
  - Verisign (for a fee)
- Private
  - Your Own (OpenSSL makes a great CA)
  - Your Employer
  - Trade/Professional Organizations
  - Your School
  - Your Country

Questions?

GEMINI
SECURITY SOLUTIONS