DNSSEC Deployment Considerations

Olaf M. Kolkman

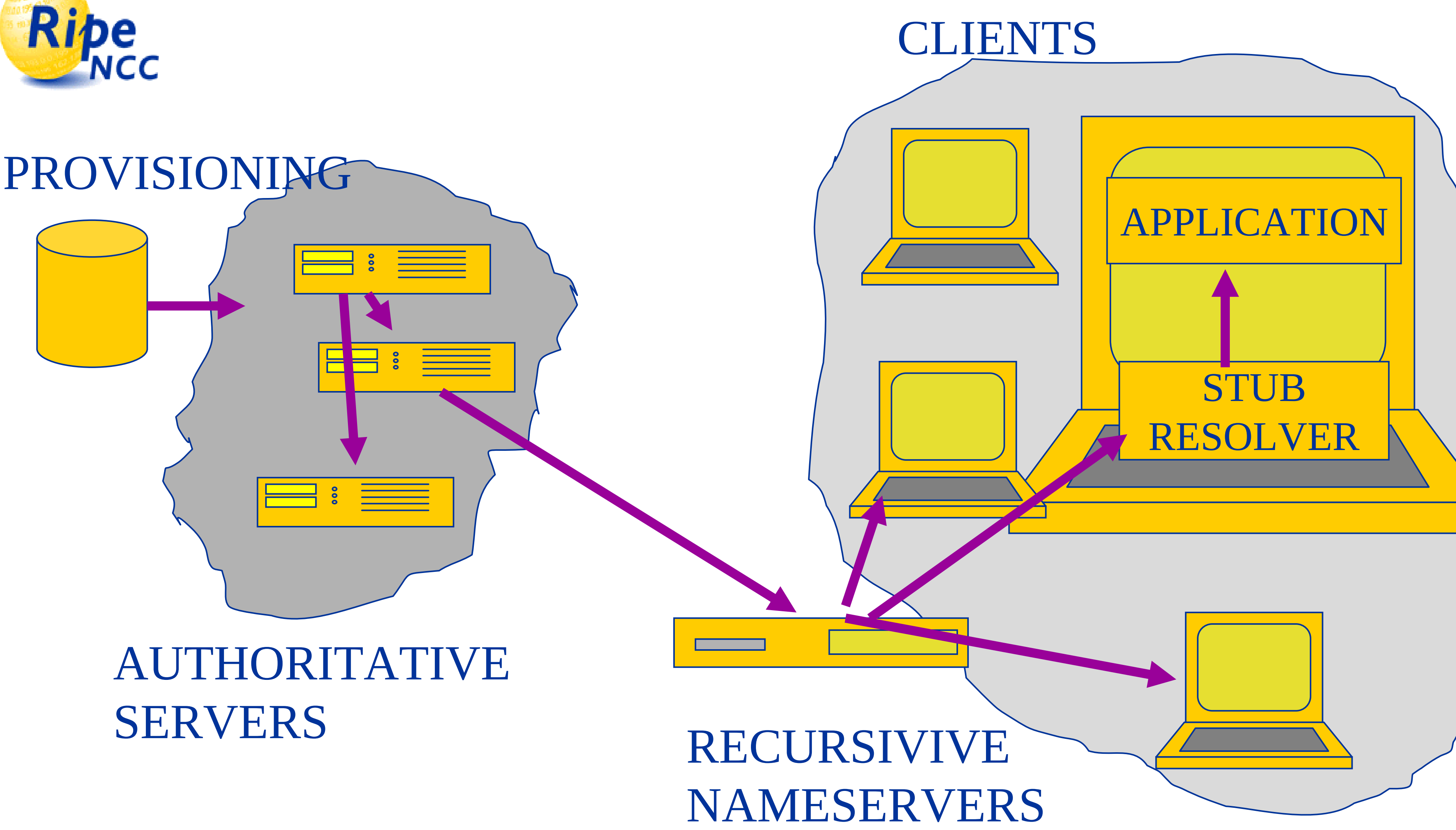
RIPE NCC

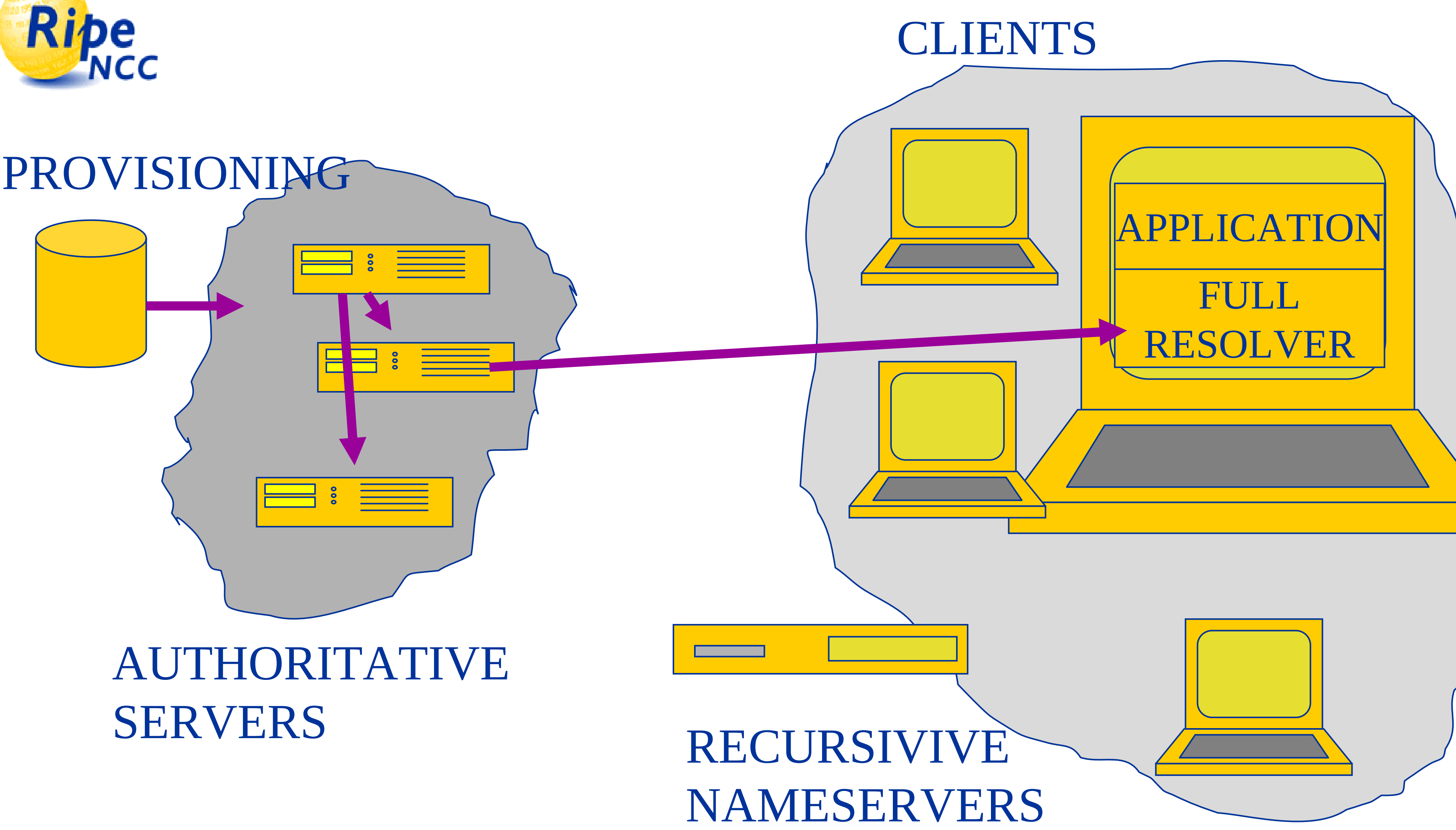
olaf@ripe.net

Goal

Using the ‘building’ blocks in the DNS architecture

- Identify where DNSSEC can be deployed now
- Identify where protocol work needs to be done
- Identify where tools are needed
- Identify possible catalysts for deployment


CLIENTS
PROVISIONING
APPLICATION
STUB
RESOLVER
AUTHORITATIVE
SERVERS
RECURSIVIVE
NAMESERVERS



CLIENTS

PROVISIONING

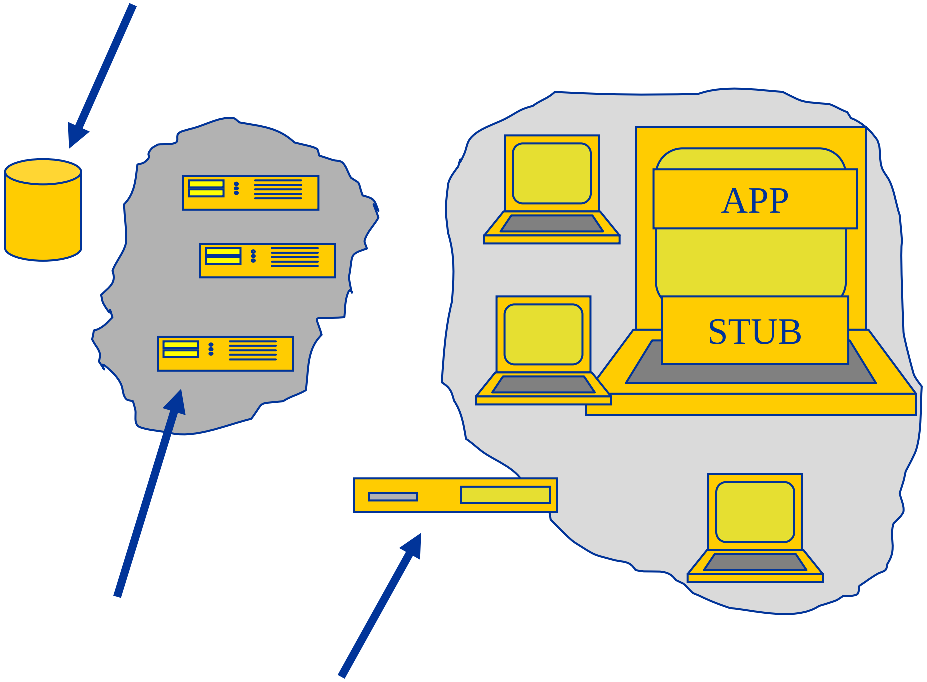
APPLICATION

FULL RESOLVER

AUTHORITATIVE SERVERS

RECURSIVIVE NAMESERVERS

DEPLOYMENT NOW
DNS server infrastructure related



Protocol spec is clear on:

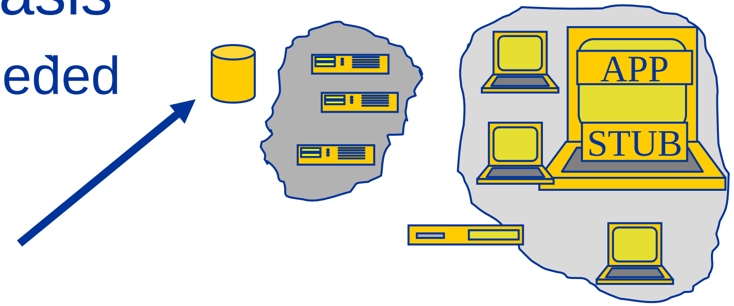
- Signing
- Serving
- Validating

Implemented in

- Signer
- Authoritative servers
- Security aware recursive nameservers

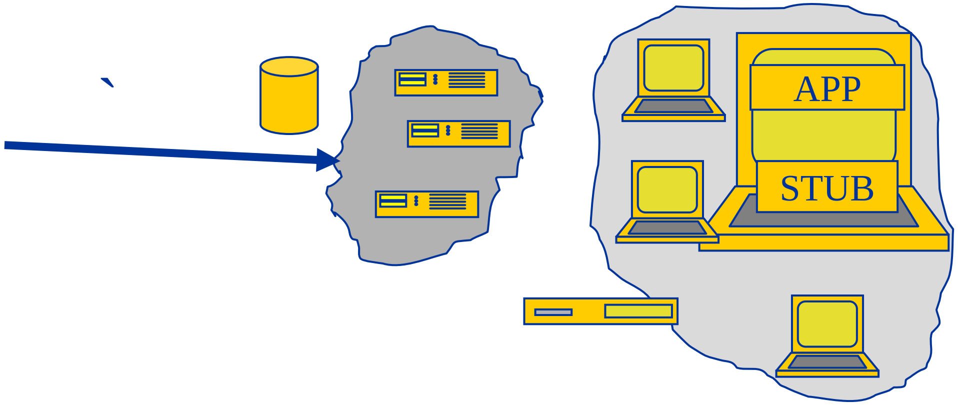
Deploying DNSSEC server infrastructure 1

- Provisioning systems
  - The signer component is readily available
  - No standard way to perform client parent key interaction (Public Key management)
    - Not really a problem, different registries use different systems
    - EPP can be extended with DNSSEC
  - Private Key management is not something most registries do on a regular basis
    - Tools and procedures are needed



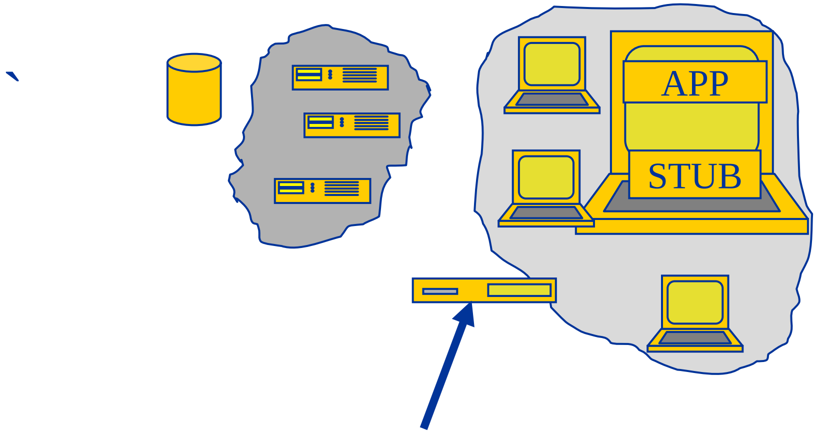
Deploying DNSSEC server infrastructure 2

- Authoritative servers
  - They will just work as long as they speak the protocol
    - Primary and secondary server infrastructure may not be under the same administrative control
    - Zone administrators eager to roll out DNSSEC may need to reevaluate their secondary servers



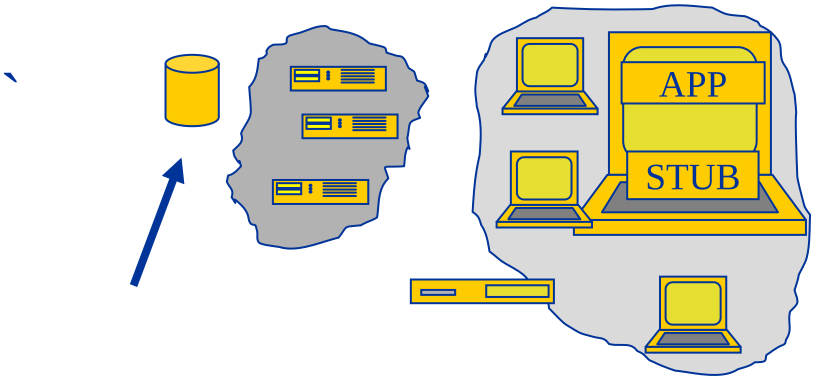
Deploying DNSSEC server infrastructure 3

- Security aware recursive servers
  - Protect the security oblivious clients behind it
    - Solves a whole class of DNS attacks
    - Either on-or-off; deployment risk
  - Multiple keys to be configured in absence of a signed root



Deploying Registry Policy

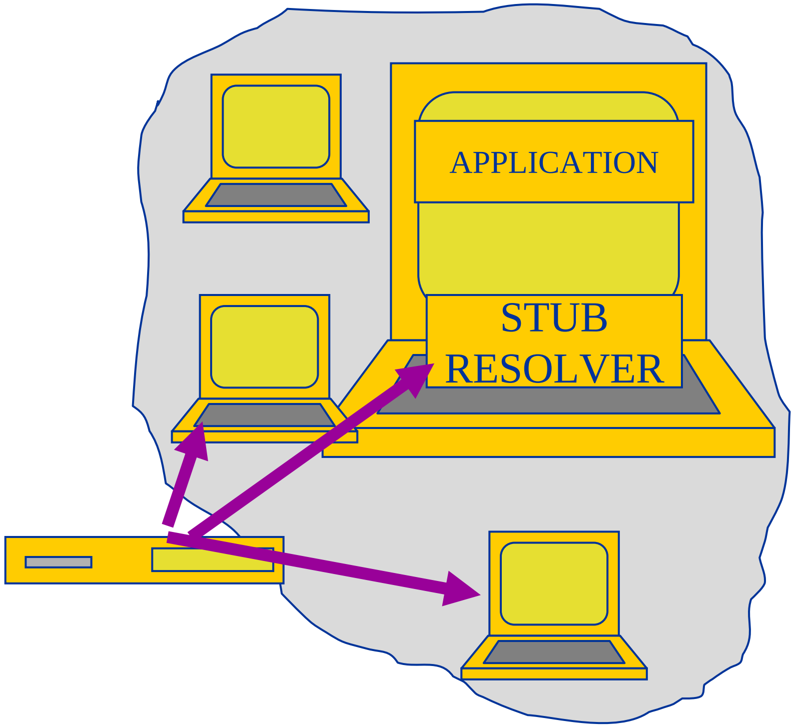
- Some registries have data transfer policies
  - NSEC walk is a barrier



The Wish List
(from DNSSEC server infrastr.)

- Public and private key management tools
- Provisioning tools
- DNSSEC aware DNS hosts
- Secure Island’s public keys distribution

DEPLOYMENT NOW
DNS client infrastructure related

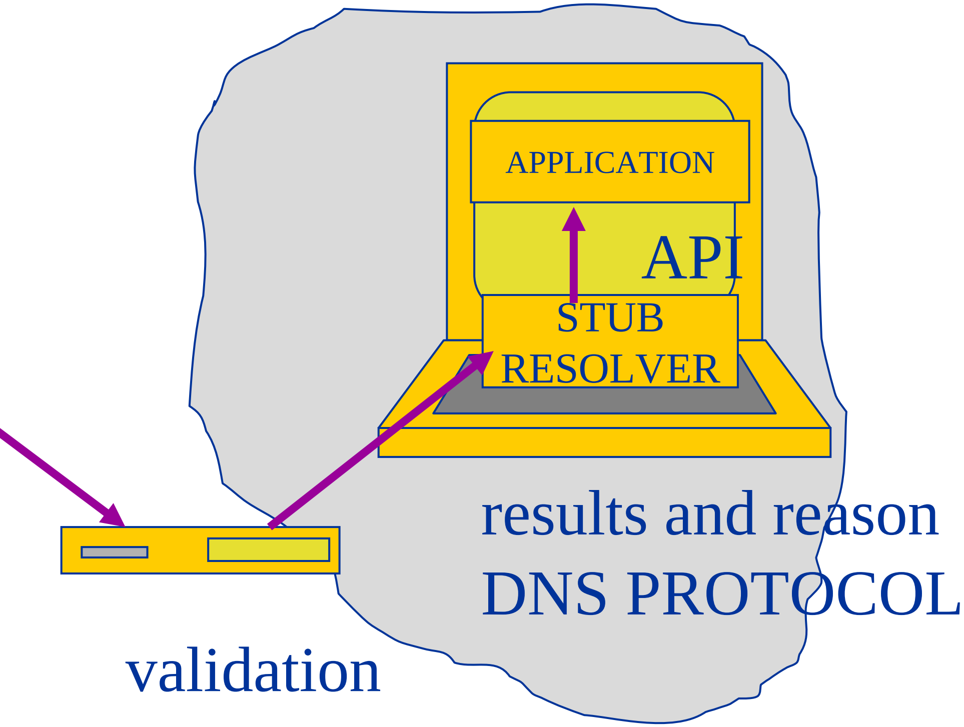


Protocol spec. lacks means to communicate policy and verification results

Current means:

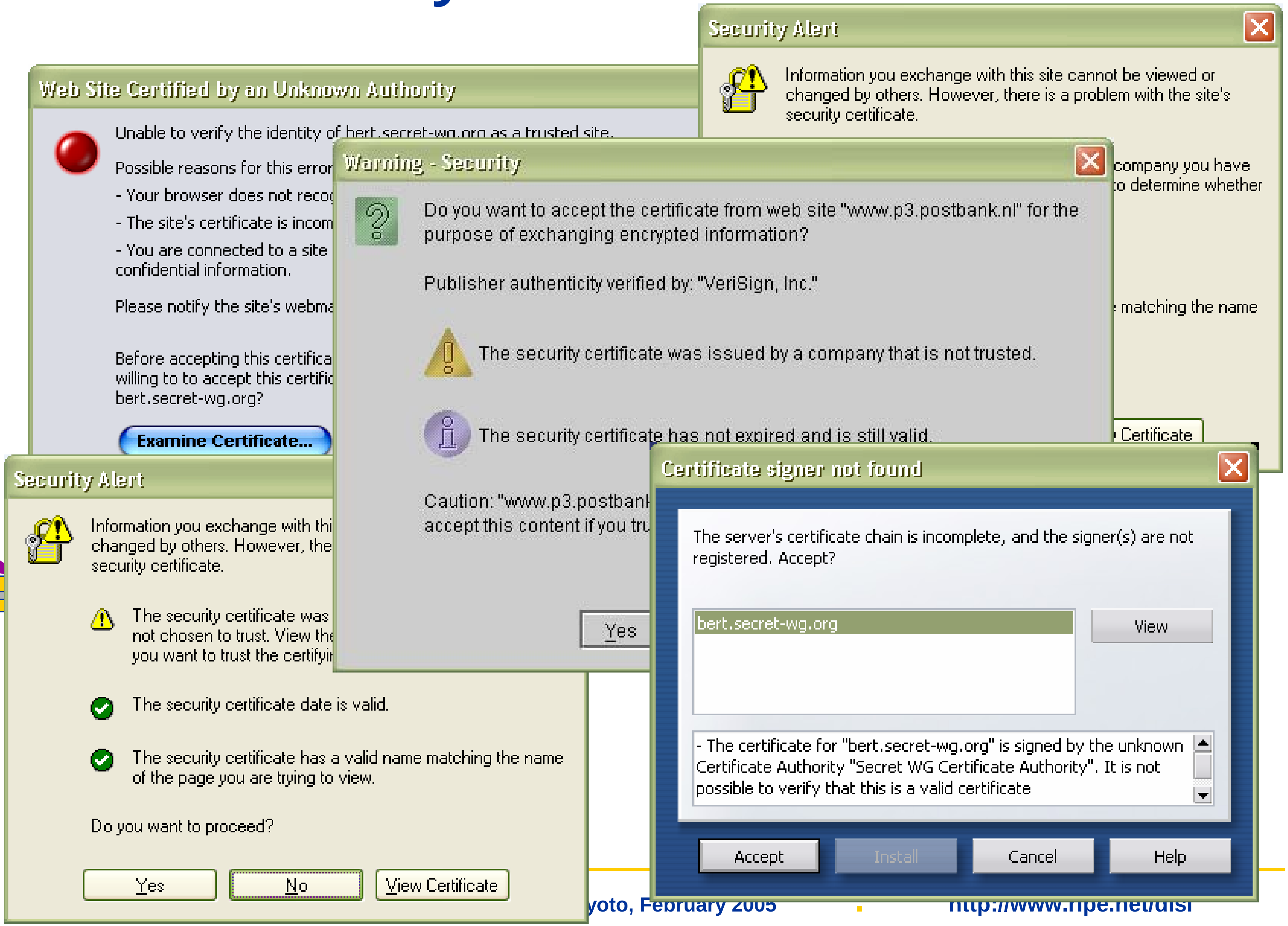
- For security oblivious stub resolvers: SERFAIL
- For security aware stub resolvers: cd bit, ad bit
- For security aware full resolvers: log files and traces

The Ideal



- The application dictates the security policy
  - An application may want to try to use the DNS data under certain circumstances
    - Signature timed out x minutes ago
    - Could not obtain key material because of network problem
    - The application uses strong crypto and doesn't care about overhead

Is this really The Ideal ????



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

company you have
to determine whether

matching the name

Certificate

Web Site Certified by an Unknown Authority

Unable to verify the identity of bert.secret-wg.org as a trusted site.

Possible reasons for this error

- Your browser does not recog
- The site's certificate is incom
- You are connected to a site
confidential information.

Please notify the site's webma

Before accepting this certifica
willing to to accept this certific
bert.secret-wg.org?

Warning - Security

Do you want to accept the certificate from web site "www.p3.postbank.nl" for the purpose of exchanging encrypted information?

Publisher authenticity verified by: "VeriSign, Inc."

The security certificate was issued by a company that is not trusted.

The security certificate has not expired and is still valid.

Caution: "www.p3.postbank
accept this content if you tru

Security Alert

Information you exchange with thi
changed by others. However, the
security certificate.

The security certificate was
not chosen to trust. View the
you want to trust the certifyi

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

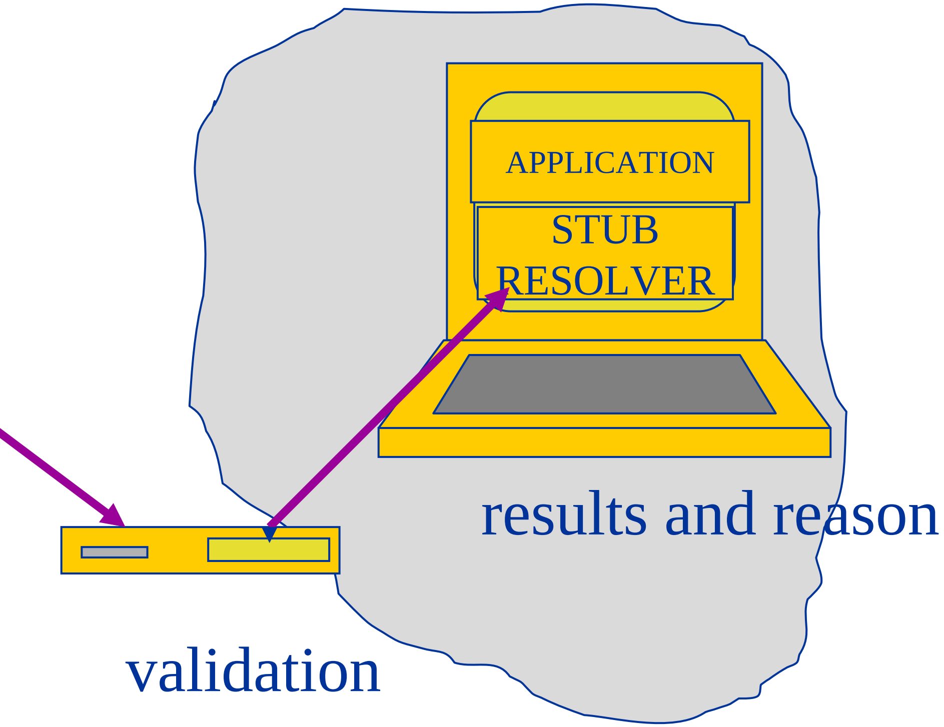
Certificate signer not found

The server's certificate chain is incomplete, and the signer(s) are not registered. Accept?

bert.secret-wg.org

- The certificate for "bert.secret-wg.org" is signed by the unknown Certificate Authority "Secret WG Certificate Authority". It is not possible to verify that this is a valid certificate

Alternatively



- Applications will come with their own resolvers
  - No standard API
  - Either validating stub resolvers
  - Or validating full resolvers

The Wish List

- *Public and private key management tools*
- *Provisioning tools*
- *DNSSEC aware DNS hosts*
- *Secure Island’s public keys distribution*
- An API and a protocol to communicate validation results
- Libraries that implement the API

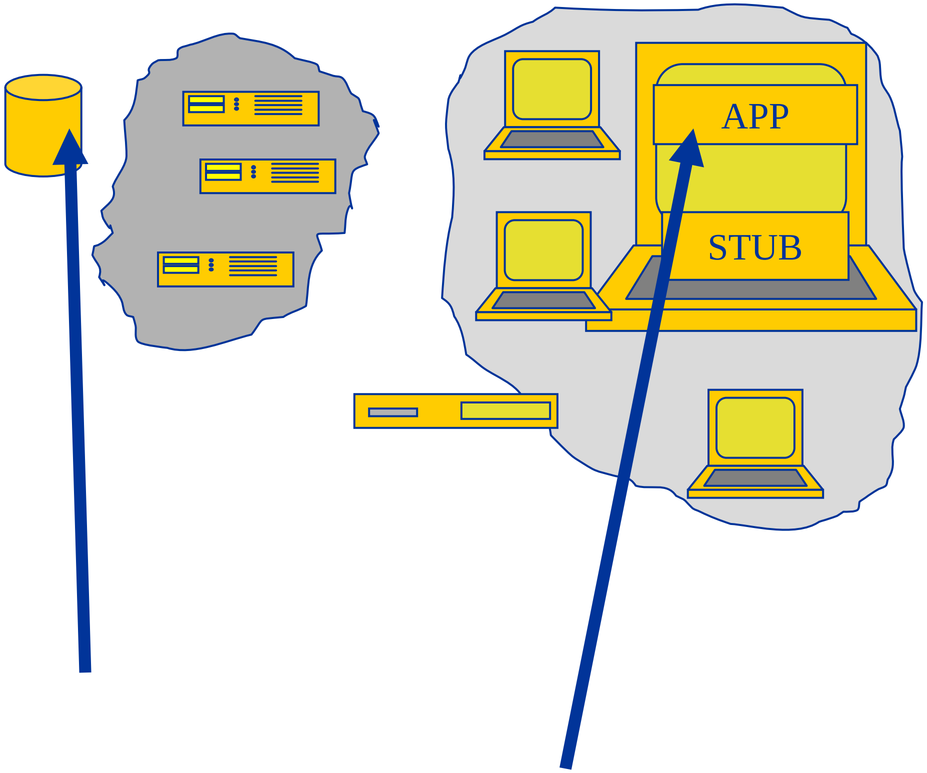
The Application
some remarks

- Why should the application make policy decisions
  - Because people are operating it; all about making informed choices.
- There may be Apps that really benefit from DNSSEC
  - DNS based anti spam tools
  - IPsec SSH and other key distribution
    - DNSSEC was not designed as PKI but the killerapp may be exploiting the PKI likeness of a secured DNS.
- The DNS Killing App, exploiting the non-secured DNS

The Wish List

- *Public and private key management tools*
- *Provisioning tools*
- *DNSSEC aware DNS hosts*
- *Secure Island's public keys distribution*
- *An API and a protocol to communicate validation results*
- *Libraries that implement the API*
- A killer App that relies on DNSSEC

Cost Benefit During initial deployment

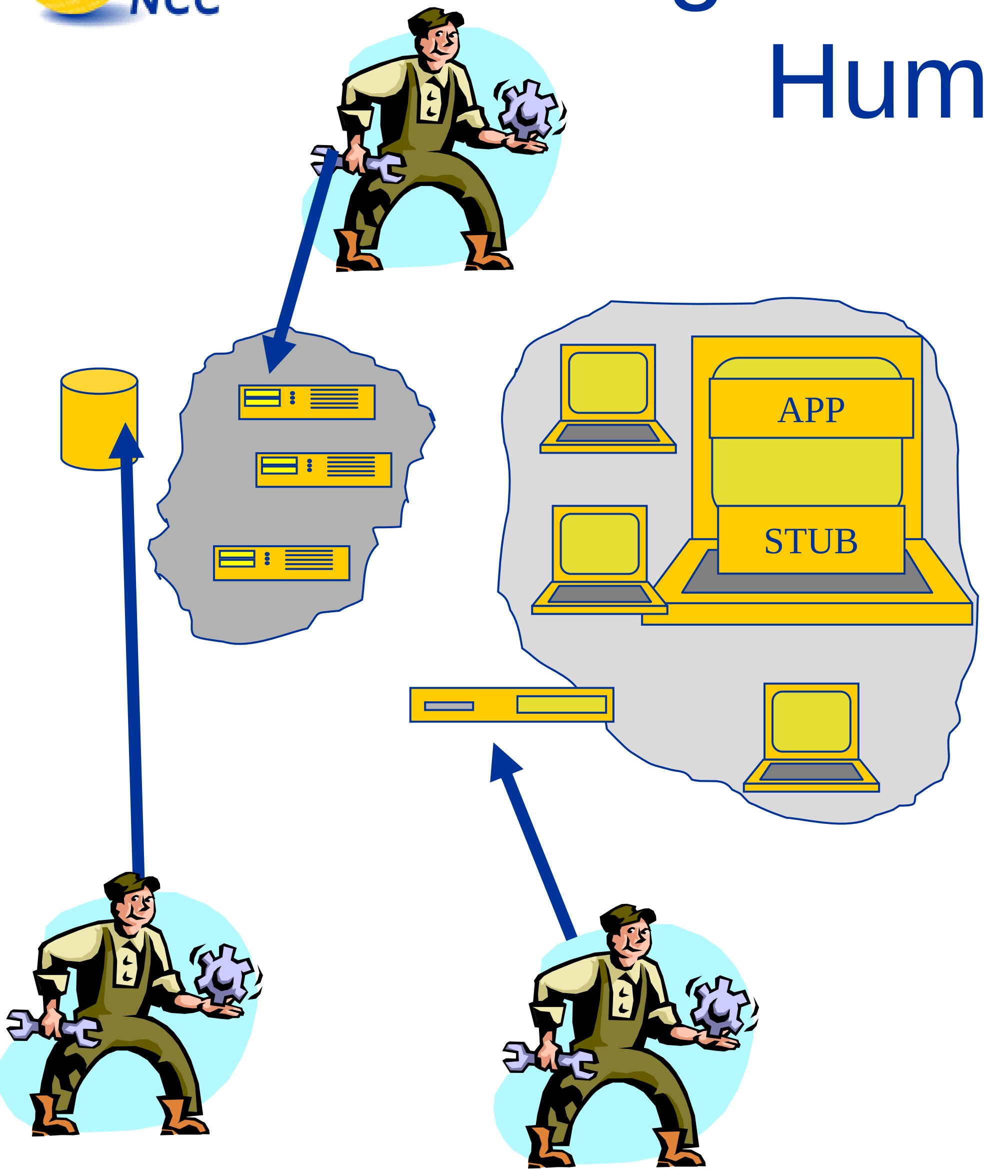


- DNSSEC will be most beneficial to the users of the applications
- Costs are on the server side
- Costs are on maintaining multiple trust anchors
- Risk for maintainer of security aware recursive nameservers

The Wish List

- *Public and private key management tools*
- *Provisioning tools*
- *DNSSEC aware DNS hosts*
- *Secure Island’s public keys distribution*
- *An API and a protocol to communicate validation results*
- *Libraries that implement the API*
- *A killer App that relies on DNSSEC*
- An incentive to invest in zone signing

Huge Cost Factor: Humans



Needed to perform the magic and keep the system running

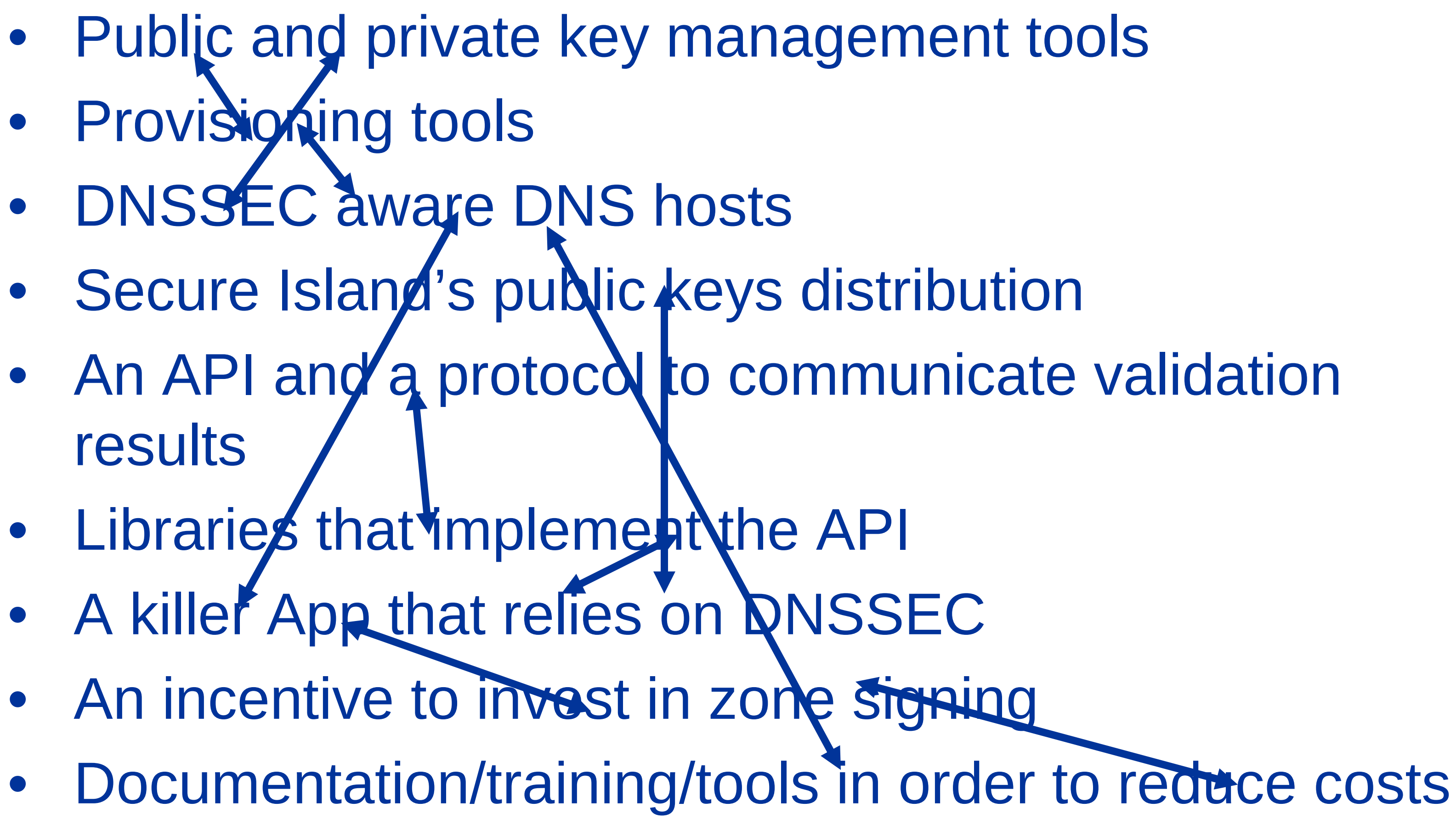
They need Clue

They need Motivation

The Wish List

- *Public and private key management tools*
- *Provisioning tools*
- *DNSSEC aware DNS hosts*
- *Secure Island’s public keys distribution*
- *An API and a protocol to communicate validation results*
- *Libraries that implement the API*
- *A killer App that relies on DNSSEC*
- *An incentive to invest in zone signing*
- Documentation/training/tools in order to reduce costs

The Wish List Interdependencies



- Public and private key management tools
- Provisioning tools
- DNSSEC aware DNS hosts
- Secure Island’s public keys distribution
- An API and a protocol to communicate validation results
- Libraries that implement the API
- A killer App that relies on DNSSEC
- An incentive to invest in zone signing
- Documentation/training/tools in order to reduce costs

Questions???

- Questions and feedback to olaf@ripe.net