



A proposal for

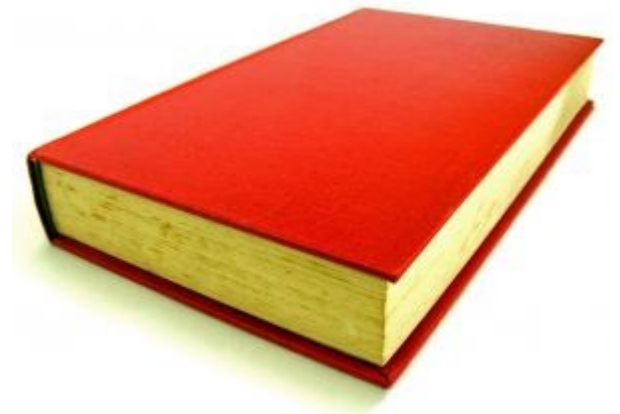
Collaborative Internet-Scale Trust Infrastructures Deployment:

The Public Key System



Outline

- Motivations
- Model Description
- Message Definition
- The PKS Node
- Federated Identities
- Considerations
- Future Work



The Objective

- Ease deployment of Trust Infrastructures based on Public Key technology in the Internet
 - X.509 PKIs
 - DNSSEC

Motivations-1

- Heterogeneous deployment environment
 - How easy is it to interact with your PKI ?
- The Need for Federated Identities
 - FBPKI, HEBCA, 4BF, TACAR, IGTF, etc.
- Many different Protocols (X509)
 - SCVP, CMP, OCSP, TAMP...
- Other Public Key Infrastructures (DNSSEC)
 - Future Infrastructures (?)

Motivations-2

- Each day we rely on Public Key technologies for online authentication
 - Web Authentication
 - Physical Authentication

No support for
Trust Infrastructures Deployment
in the Internet

Current Needs Demand Solutions...

- DNSSEC to distribute certificates
 - Trust does not follow DNS hierarchies
 - Organizational Problems (DNS vs CA)
- Computing Grids TA distribution
 - Ad-Hoc TA distribution
 - No interoperability

Message to take away...

We need a **standardized, scalable** and **interoperable** system for PK support for the Internet

So far... It's been a Bumpy Ride!



Problem-1

- No Globally Authoritative Infrastructure
- No easy Interaction with different Infrastructures
 - PKI Resource Query Protocol (PRQP)

A Public Key System is needed to allow PK-enabled applications to discover and easily use resources offered by different Authorities

Problem-2

- Interaction with different parts of a PKI is difficult
 - Many Different PKI Protocols
 - Many Different Transport Protocols
 - HTTP, HTTPS, FTP, etc.
- Applications and Certificates
 - renewal, revokation

A Public Key System that mandates for a simple transport protocol capable of routing all current and future PKI messages

Problem-3

- Lack of *contextual trust*
 - Classes of trust (eCommerce, eBanking, eMail)
 - Easy Trust Anchor Management
- Mobile devices
 - Local trust in home environment

A Public Key System that provides the ability to group TA according to specific environments to help users manage (or delegate) trust settings.

Problem-4

- Lack of support for federated identities
- Need to know if a CA/PK is part of a federation
 - Computing Grids, DNSSEC, etc.

A Public Key System that eases the deployment of federated identities by facilitating a method for disseminating information about which organization or federation use/include/trust a specific TA.

The Challenge

To provide a flexible support system for Trust Infrastructures deployment

.... S0 ...

(very dramatic pause...)

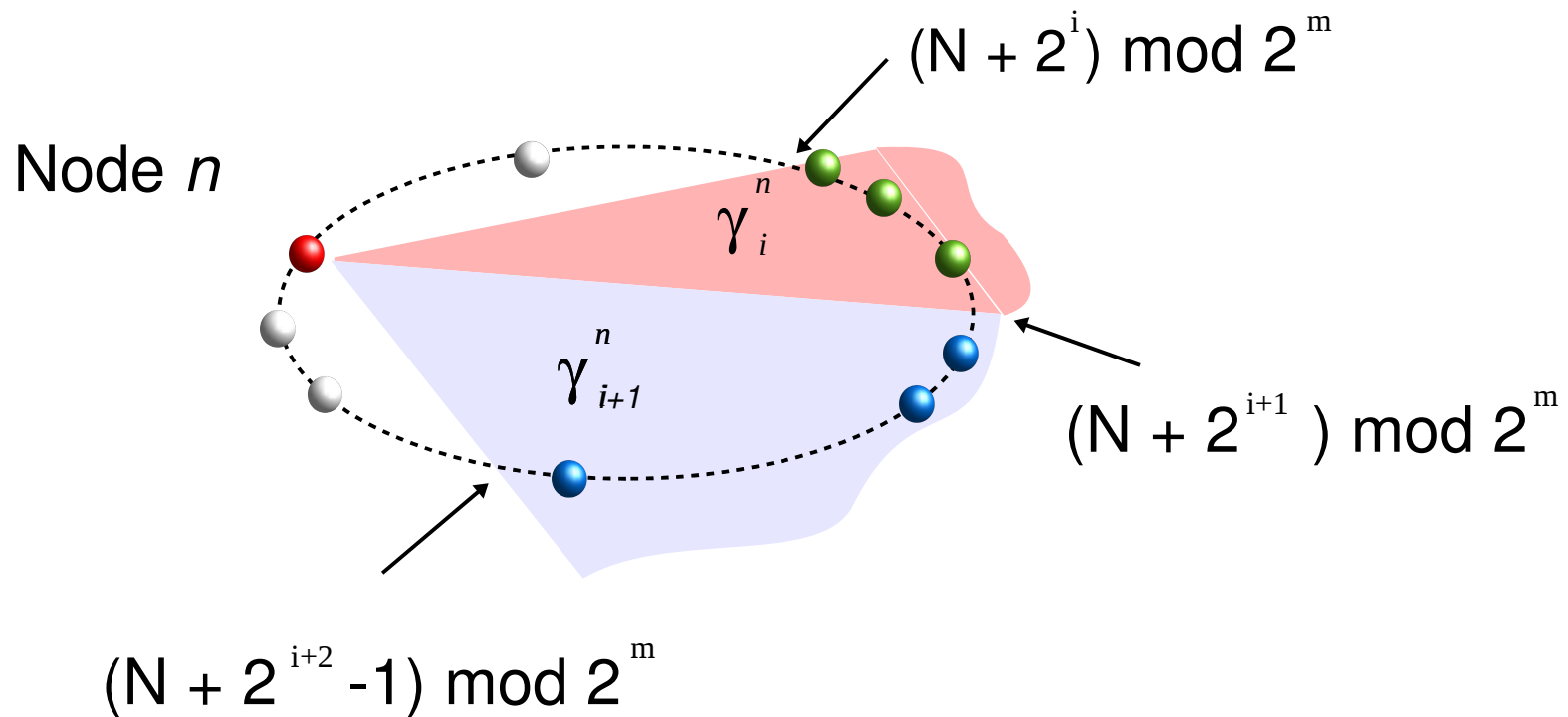
The Public Key System

- A system to support current needs for Trust Infrastructures (TI) deployment
 - Addresses the aforementioned problems
 - Increases Interoperability among TI
- Supports Public Key systems
 - Algorithm(s) agile
 - Backward compatible with deployed TI
- Internet Oriented
 - Scalability

The Public Key System (PKS)

- Peer-to-peer system based on DHT [Chord]
- Simple Operations
 - lookup()
 - join()
- Identifiers based on hash(PK) [PEACH]
 - m = bits hash function
- Each node keeps a lookup table
 - m entries

The Public Key System (PKS)



DHT Basics

- ID space hash(x)

$$\forall i \in [1, 2, \dots, m], \Rightarrow x_i^n = (id_n + 2^i) \bmod 2^m$$

- Lookup table $n \Rightarrow id_n < x_i^k$

$$\gamma_i^n = [x_i^n, x_{i+1}^n)$$

- Lookup in $O(\log(m))$

The Public Key System (PKS)

- n-th node lookup table

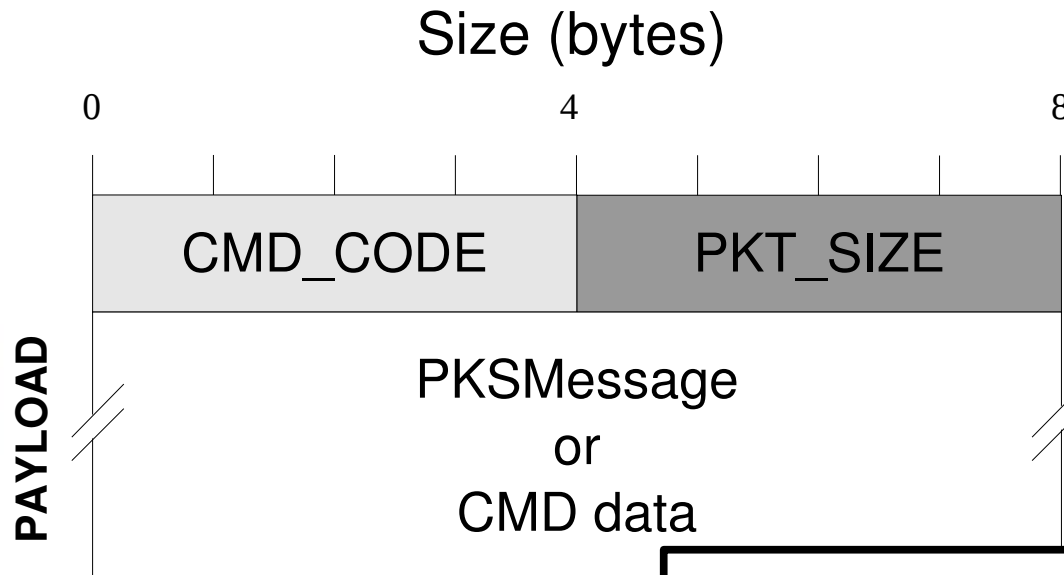
$$x_0^n = (id_n + 2^0) \pmod{2^m}$$

⋮

$$x_m^n = (id_n + 2^{m-1}) \pmod{2^m}$$

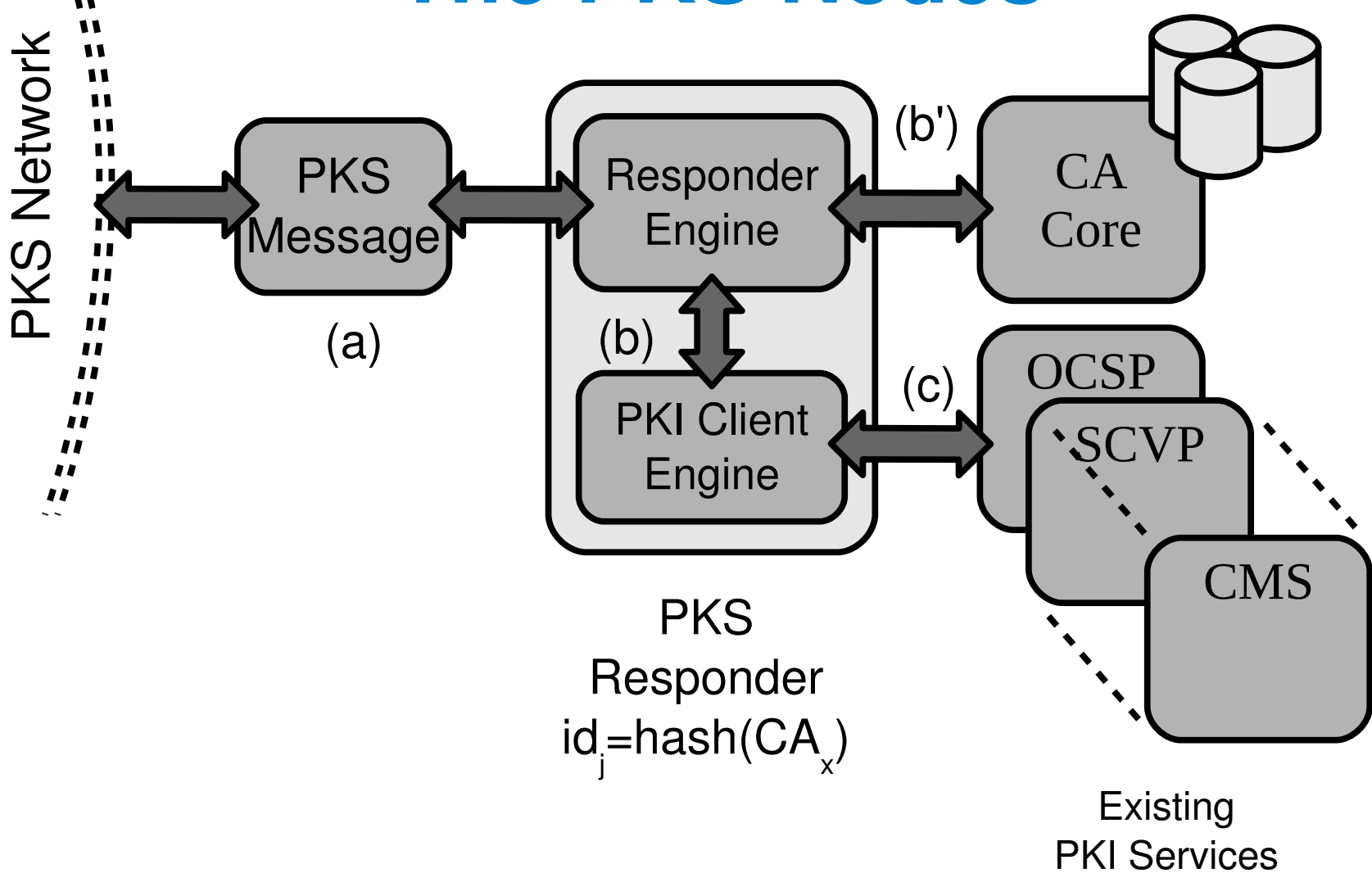
The PKS Message Format

Simplified Message System



```
PKSMMessage ::= {  
    protocol      OBJECT IDENTIFIER,  
        --- Identifier for the data protocol  
    targetNode    OCTET STRING,  
        --- Target Node Identifier (hash)  
    rawBytes      OCTET STRING  
        --- Binary data (e.g., CMS message)  
}
```

The PKS Nodes



Federated Identities

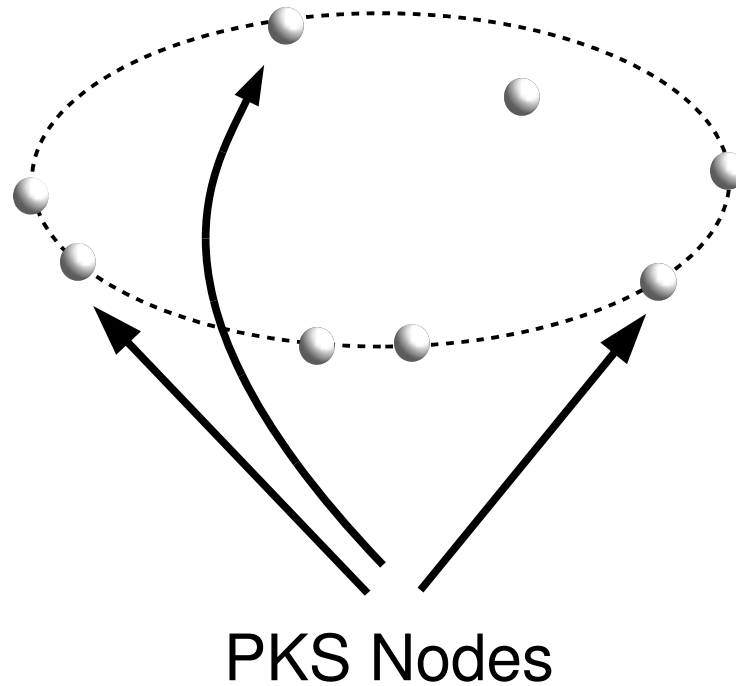
- PKS Federation Authorities (PK-FA)

$$id_j = hash(x_j)$$

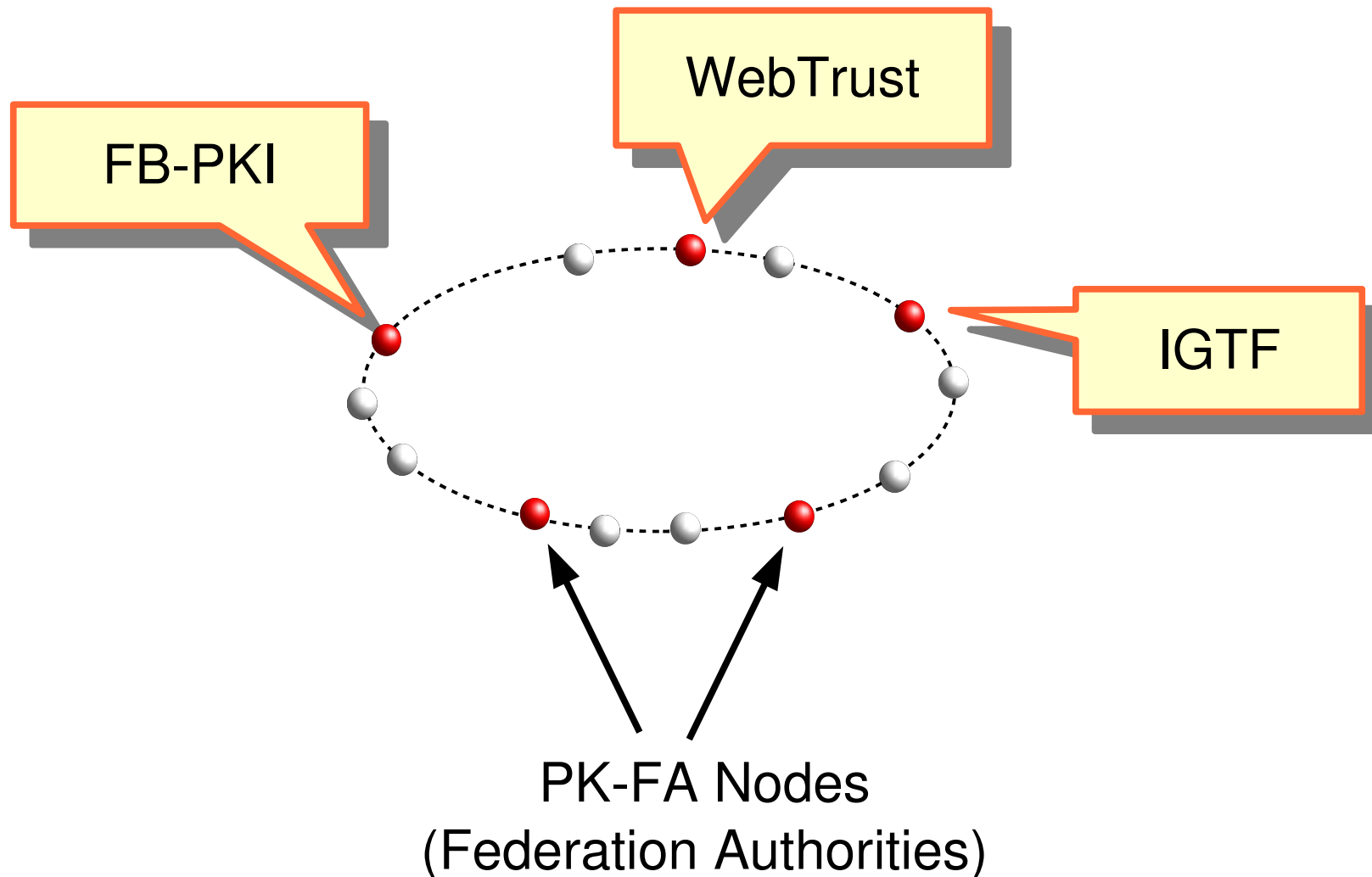
- PK-FA provides responses to client about a CA being part of a federation
 - Is this CA part of the Federal Government ?
 - Is this user's certificate part of TACAR ?
 - Is this certificate for an Internet DNS server ?

Extending the PKS Network

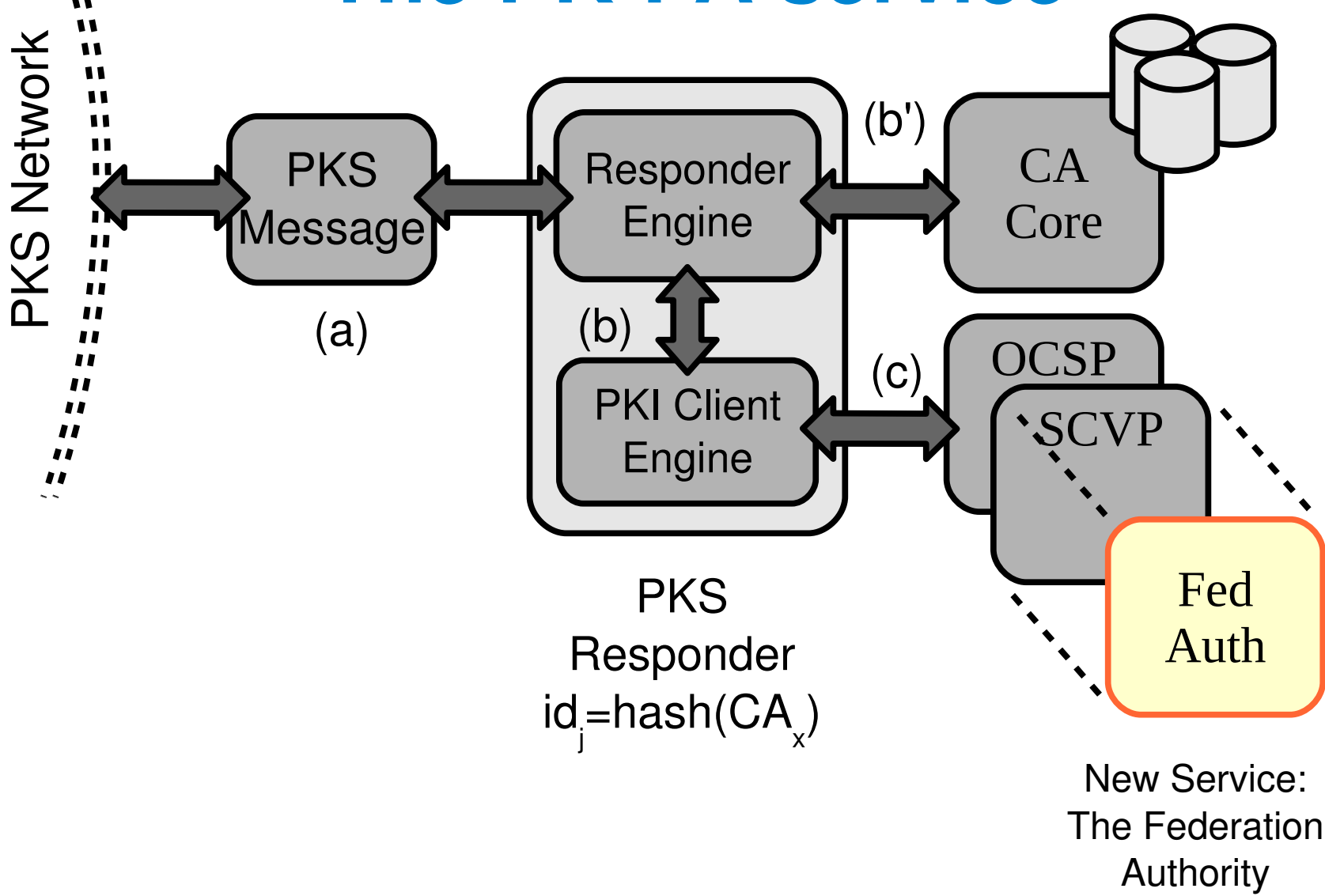
Let's add a new class of Nodes to the PKS network



Extending the PKI Network: Federation Authorities



The PK-FA service



Classes of Federations

- Hierarchical Federation Infrastructure
- Class Federation Authorities
 - Identifiers based on PK (not certs)
 - Local, Internet, Network, Organization, and Application
- Deployment of Trusted Keys for primary DNS domains
 - “.”, “.edu”, “.net”, “.org”, “.com”, etc.
 - Keys for “.” can be used/revoked/replaced

Conclusions

- We rely on PK technology
 - Digital IDs
 - Passports
 - DNSSec
- We need a Public Key System capable of supporting the use of PK on the Internet
- We proposed a PKS and a possible deployment design based on a collaborative approach

Future Work

- Deploy the system in a test bed
- Study attacks to the PK network
 - Malicious nodes, etc.
- Define an API for providing access to the PKS for:
 - Easy integration with existing OSes and Apps
- Publishing an I-D at IETF for consideration within the PK-NG WG (IRTF)

Contacts, Questions, etc.

- Email:
 - Massimiliano Pala <pala@cs.dartmouth.edu>
- Website:
 - <http://www.openca.org/projects/ng/>