Key Centric Identity and Privilege Management

Paul A. Lambert

Marvell Semiconductor, Inc.

Overview

- **Privilege Management in ICSG: “who can do what”**
- **Problem Statement and Target Markets**
- **PMP Overview**
- **Key Centric Overview**
- **Syntax**
- **Example Key Centric Statements**

Privilege Management Protocol Working Group in IEEE ICSG

- Define protocols for efficient authentication and the secure determination of "who can do what".
- The "who" is a cryptographic based identity that supports authentication and key establishment.
- The "what" consists of the manageable attributes of a system.
- The enforcement decisions are based on policy rules that define the relationships of entities to the manageable attributes.

http://standards.ieee.org/develop/indconn/icsg/pmp.html

Paul A. Lambert**, Marvell**

Target Applications

- **Wireless peer-to-peer communications**
- **Sensor networks**
- **Smart grid (wireless access fro control and sensors)**
- **Health care (security for wireless health care devices)**
- **Automotive and smart highway applications**

Target Work – Privilege Management

- **use existing cryptographic definitions (like Suite B, and pick one default suite)**
- **selection of authentication exchange from existing standards**
- **definition peer-to-peer authentication exchange based on above selections**
- **suitable for peer-to-peer strong authentication and key establishment**
  - include capabilities for role definition and determination
  - provide framework for message authentication
  - above must have relatively efficient bit encoding

What is Privilege Management?

- **In complex systems, mechanisms are required to securely manage "who can do what"**
  - "Who" needs to be a identity that can be securely authenticated
  - "Do What" needs to be a flexible description that securely carries descriptions of manageable attributes of a system
  - The decision needs to be based on "Policy Rules" that relate the identities to attributes in a humanly manageable fashion

Simple Example Use Case

- **Smart Grid – Management of devices in a home**
  - A individual home owner should be able to read and set a home thermostat, air conditioner and appliance settings in a house.
  - The power company may provide incentives to the home owner if some appliances can set to reduce consumption
  - Control of this “privilege management” must be “secure”

Privilege Management Requirements

- **Secure**
  - Data origin authentication (cryptographic)
  - Data integrity
  - (modification of policies or attributes can be detected)
  - Data Confidentiality (encryption of some data transfers)
- **Efficient**
  - Target devices include embedded systems (e.g XML or SOAP are not appropriate protocols)
- **Flexible Schemas**
  - Needs to allow extensions for many types of “schemas” (example SNMP, or PICS)

Current Issues with Privilege Management

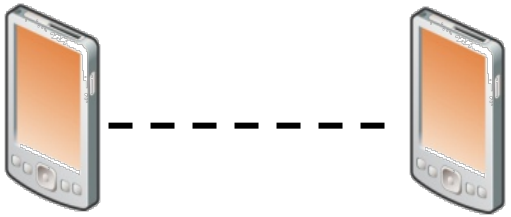
- **There are frameworks, but no adequate protocol solution to carry privilege management**
  - XML based solutions are not efficient
  - Inadequate policy description languages
    - Poor mapping of syntax to semantics

Proposed Solution

- **Protocol Standard to Support**
  - Peer-to-peer authentication messages
    - (based on existing cryptographic standards)
  - Efficient flexible attribute representation
    - SNMP-like with clear semantics
    - Secure transport (use existing digital signature standards)
  - Policy description
    - Relate identities to attributes
    - Include symmetric component (PICS-like) to support easy management interfaces
- **Inspiration and References:**
  - HIP, SDSI/SPKI, YAML, RT (John Mitchell et al), SecPAL, OASIS XACML protobufs (Google)

Strong Device-to-Device Authentication

- **IEEE 802.11 does not have a "good" solution for device-to-device authentication**



- **Preshared keys are problematic:**
  - Difficult to install
  - Poor authentication (can be reshared)

- **EAP based methods are designed to use a remote server**
  - Difficult to configure
  - Few APs have built in server (one approach for perr-to-peer)

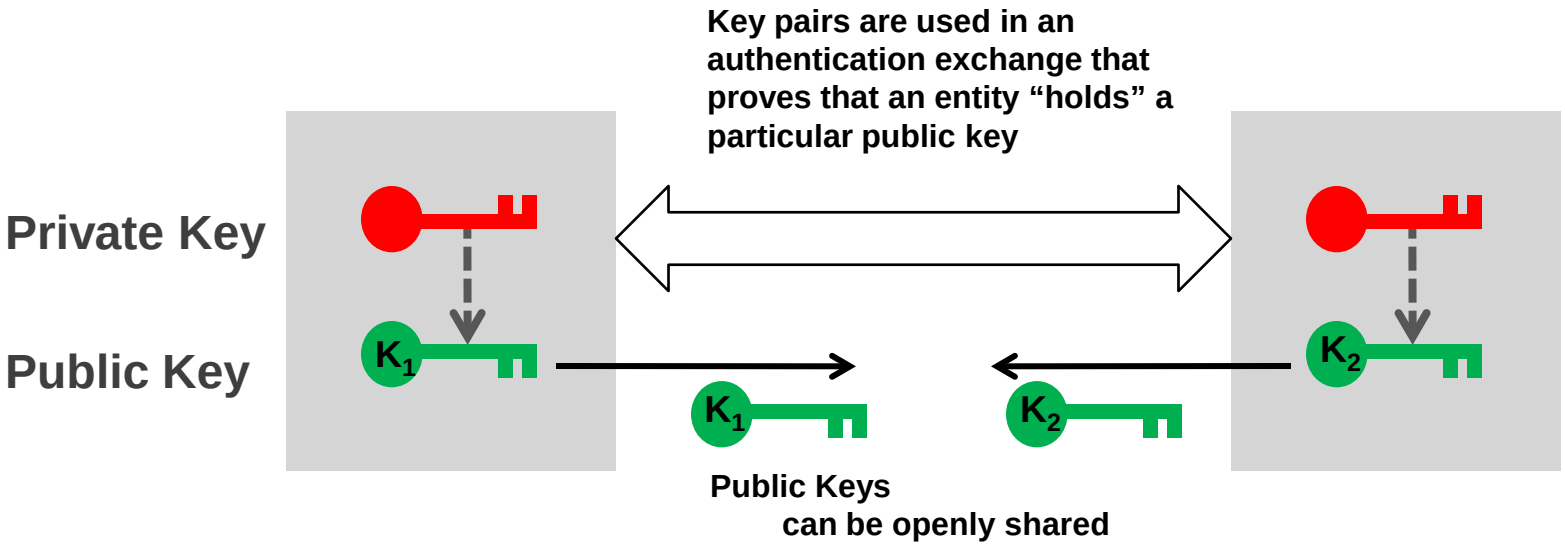
Device-to-Device Authentication Possible Use Cases and Benefits

- **Simplified secure device discovery**
  - All devices have an provable identity
  - Enables good peer-to-peer security
- **Easy device enrollment and installation**
  - Provable identity greatly simplifies installation process
  - Simplified installation of headless devices (sensors, etc)
- **Cost and complexity reduced for systems needing centralized authorization**

Proposed Framework

- **Every device has a public / private key**
  - public key is used as identity
    - Raw key or hash of Key
    - Certificate, but not always requiring a Certificate Authority
      (CA's assign names – this is not necessary)
- **Simple Key Exchange**
  - Preassociation in 802.11
  - 4 message exchange
  - True peer-to-peer (either side can initiate)
  - based on well defined cryptographic standards
    (a few to choose from – ANSI, etc.)
  - Able to support Suite B

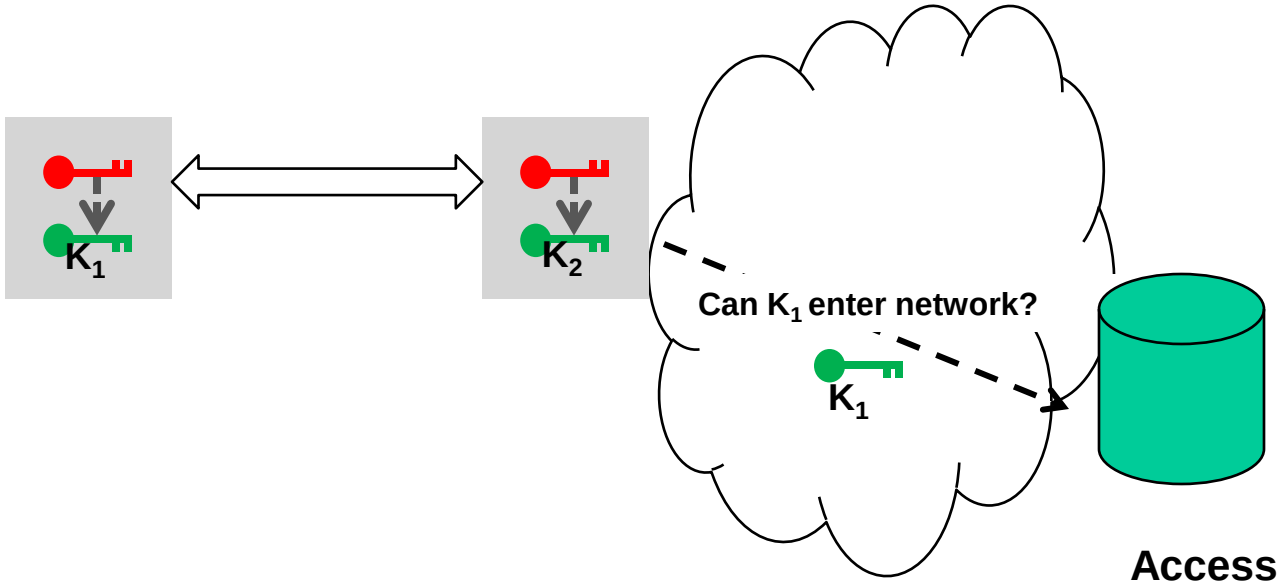
Public Key Based Authentication



Simple Device Enrollment

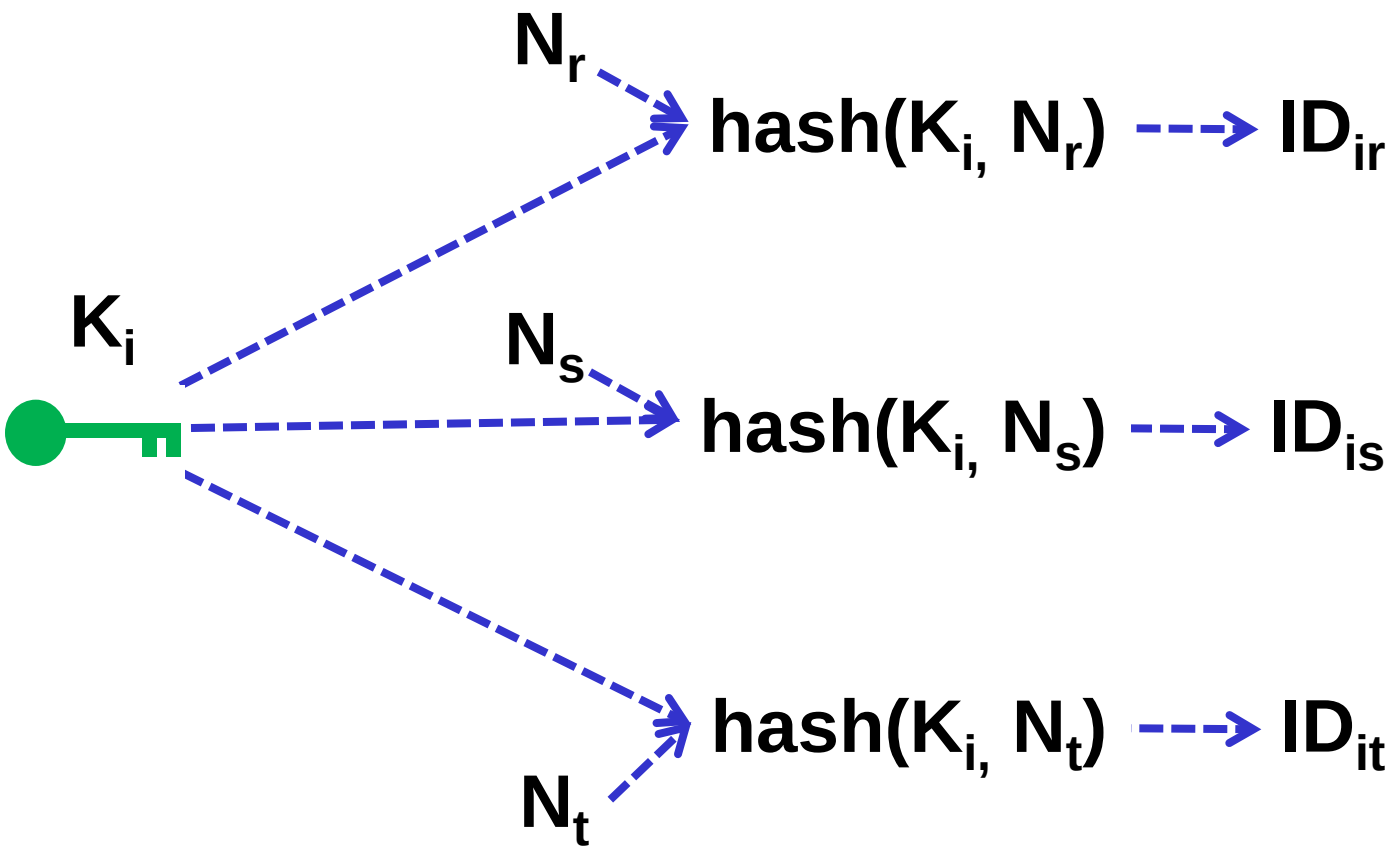
- **Devices have a identity out-of-the box**
  - Self generated key pair
  - Binding of wireless authentication to a specific device
    - Label based on public key
    - Remote enrollment based on knowing identity

Scalable Access Authorization
Key Centric Access Control



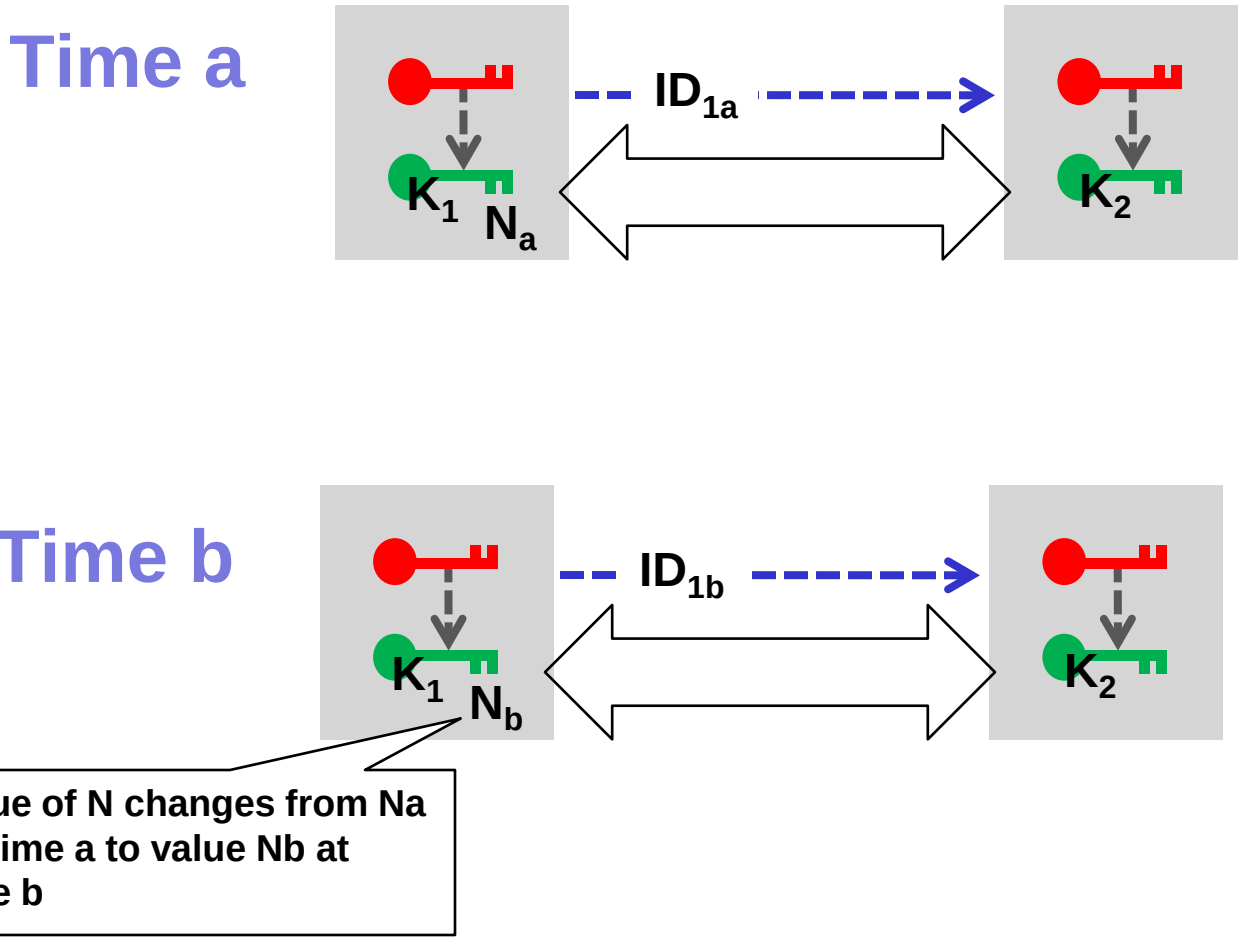
Access control servers do NOT need to hold any secrets

Multiple IDs from the same Public Key



Paul A. Lambert (Marvell)

Changing Visible ID over Time



Hashing Keys to Form Addresses

- **Public keys can be used as an address using a hash**

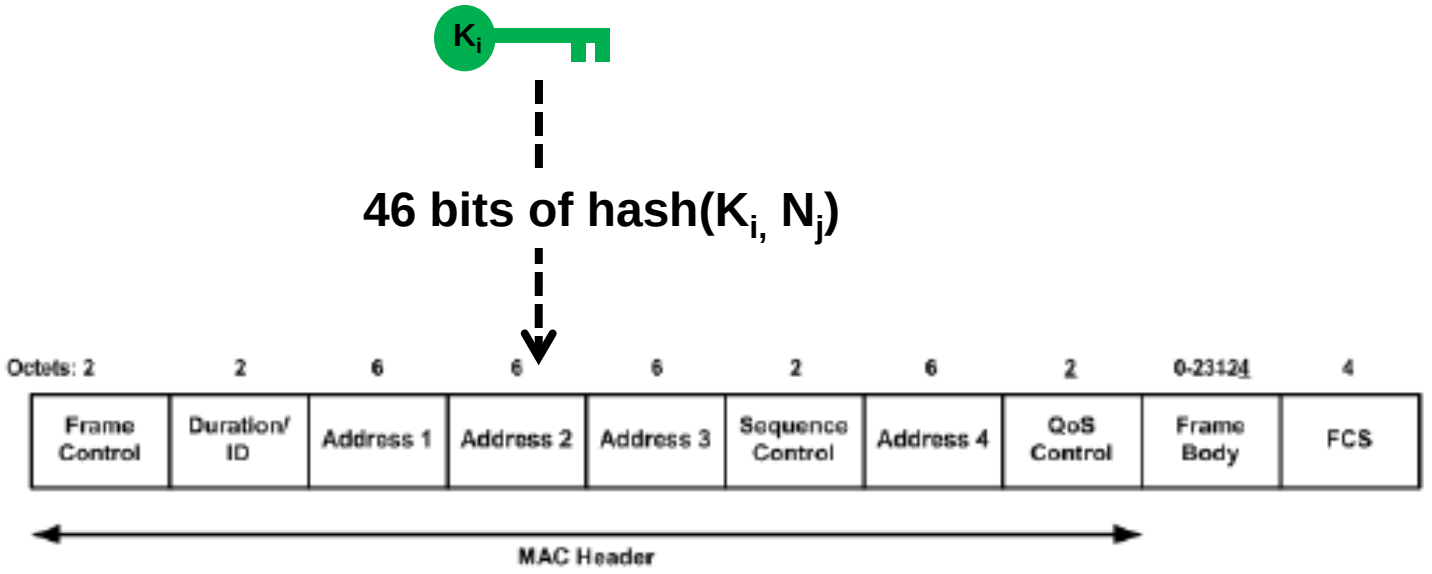


Figure 7-1—MAC frame format

Syntax – Comparison

Syntax	Protocol	Binary Efficient Encoding	Human Readable
ASN.1	PKIX	**Yes**	**No**
XML	W3C DSIG	**No**	**No**
S Expressions	SDSI / SPKI	**No**	**No**
YAML + binary encode	PMP	**Yes**	**Yes**

Paul A. Lambert**, Marvell**

YAML Based Syntax

YAML is very readable

YAML can have 1-1; readable-to-binary encoding

- Each tag assigned a type encoding

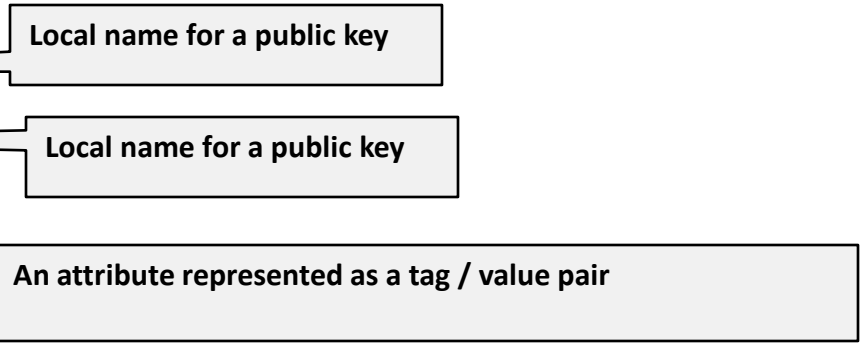
```
---
invoice: 34843
date   : 2001-01-23
bill-to: &id001
    given  : Chris
    family : Dumars
    address:
        lines: |
            458 Walkman Dr.
            Suite #292
        city    : Royal Oak
        state   : MI
        postal  : 48046
```

PMP Statements – Simple Example

Use Case Example:

“Alice says Bob has label foo”

```
---
says: *alice
this: *bob
has:
    - label: foo
---
```



PMP Statement Examples - Keys

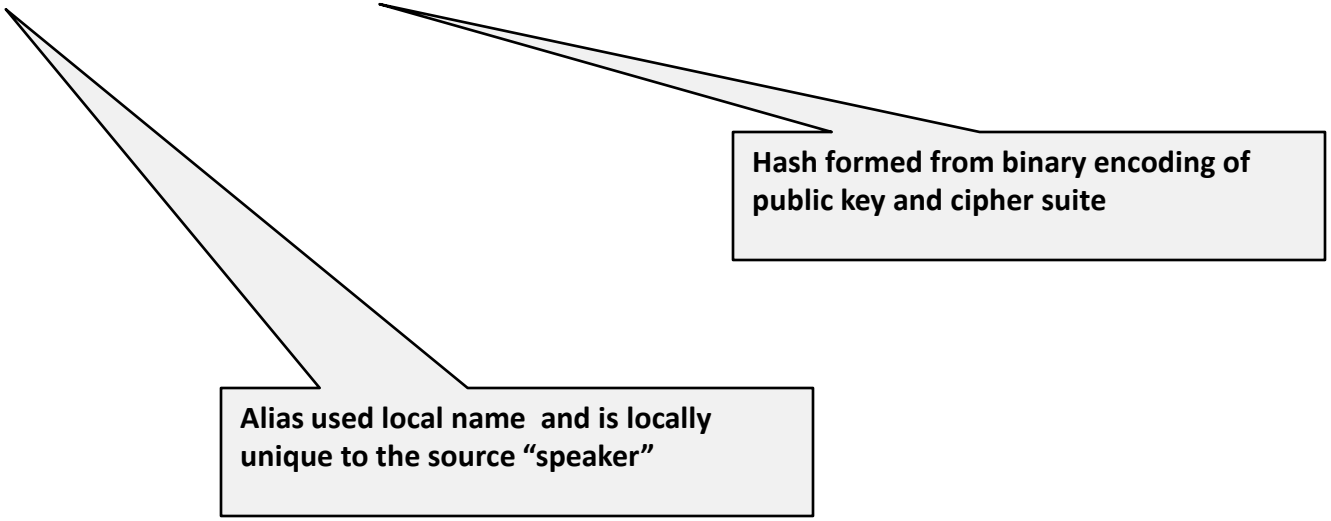
```
# A Statement with just a key and (cipher suite, keyId)
   binding
---
keyId: &alice
   0xe9a7e7badcb66ee13643c848e6d981523a08d2268eab7df259efee8a7
   f910595
cipher suite: suite Z
key: 0x254b6d0007da66b3d99505a04bd9444c\
       6bd5388e2154a3c38173bc32d46e609c\
       b8a44637c2f7c653dc18a7c63cf73829\
       a71c7f0009100ef866309ed1f069f4a6\
       108ac3f81637
---
```

"cipher suite" is a collection of algorithms and defines key size and appropriate algorithm fo defined usages of keys (encryption, signing, hash, etc.)

Example - Binary encoding of ECC public key parameters. Each parameter could be called out with tag, but not all that relevant to human readability

PMP Statement Examples - Alias

```
# A statement containing 6 keyIds and local alias
---
keyId: &alice  0xe9a7e7badcb66ee13643c848e6d981523a08d2268eab7df259efee8a7f910595
keyId: &bob    0x22659efee8a7f910595e9a7e3a08d8eab7df243c848e6d98157badcb66ee1362
keyId: &carol  0x43c848e6d981559efee8a7f910595e9a7e7badcb66ee13623a08d2268eab7df2
keyId: &alice1 0xdcb66ee13623a08d2268eab7df243c848e6d981559efee8a7f910595e9a7e7ba
keyId: &alice2 0x59efee8a7f910595e9a7e7badcb66ee13623a08d2268eab7df243c848e6d9815
keyId: &alice3 0x8d2268eab7d6ee13623a0f243c848e6d981559efee8a7f910595e9a7e7badcb6
---
```



PMP Statement - Assignment

```
# a constrainted attribute assignment using “while”
# note that “has” is a sequence value using the ‘-‘ and may
# have multiple assigned tag value pairs
---
says: *alice
this: *carol
has:
    - dns address: foo.bar
while:
    - time interval:  2012-06-21 to 2013-06-22
---
```

Using SDSI/SPKI terminology. Typical application would have this statement signed by Alice (not should to focus on statement types)

DNS used as an example that has well know charateristics. Other attribute tag could be: group, label, name, etc.

PMP Statement - Delegation

```
# delegation of trust for a single attribute type/range
# using the “trust for” tag
---
says: *bob
this: *alice
can say:
    - dns address range: *.bar
while:
    - time interval:  2012-06-21 to 2014-06-22
---
```

Delegation of ability to “speak” within a certain attribute range

“dns address range” is corresponding range object for “dns address” attribute

PMP Statement – Cloning and Revocation

```
# A full transfer of trust from one key to another
---
says: *alice
this: *alice1
trust same as: *alice
---


# Revocation of prior trust
---
says: *alice
revoke trust:
    - this: *carol
---
```

Questions?