Constrained voucher

draft-ietf-anima-constrained-voucher-09

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 109
ANIMA Working Group

Constrained voucher

BRSKI uses EST, HTTP and TLS

This draft proposes

- constrained voucher additions to voucher and use of SIDs
- Extends coap-est draft with BRSKI extensions to EST
- CoAP, CBOR, CMS, and COSE

to support voucher transport for constrained devices

EST: Enrollment over Secure Transport
BRSKI: Bootstrapping of Remote Secure Key Infrastructures
SID: YANG **S**chema **I**tem i**D**entifier

COSE: CBOR Signing and Encryption (RFC 8152)
CMS: Cryptographic message Syntax (RFC 5652)
CBOR: Concise Binary Object Representation (RFC 7049)

Modifications

rt =“brski” extends rt=“est” of est-coaps

The use of /.well-known/brski will be supported like /.well-known/est

All cose cbor examples have been copied from running implementations running a full BRSKI enrollment scenario:

- Client <> Registrar
- /brski/rv
- /brski/vs
- Registrar <> MASA
- /brski/rv
- /brski/ra

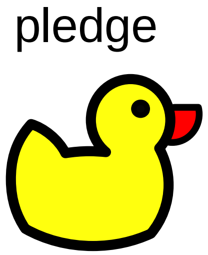
Discussion

- Is CMS-signed-CBOR signing useful next to COSE-signed-CBOR signing?
- Use of `proximity-registrar-subject-public-key-info`
- Do we need a CoAP version of Registrar/MASA interaction?
  - + Beware: MASA should support CoSE-signed-CBOR vouchers which are directly sent back to pledge

Thanks to weekly discussions in BRSKI design team on Thursday

Discussed options for Registrar/MASA interaction
Use Same Format as received

Discussed options for Registrar/MASA interaction
Use Same Format as received



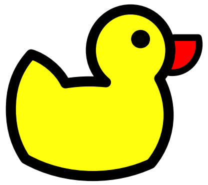
Discussed options for Registrar/MASA interaction
Use Same Format as received

pledge

Registrar

Discussed options for Registrar/MASA interaction
Use Same Format as received

pledge



Registrar

MASA

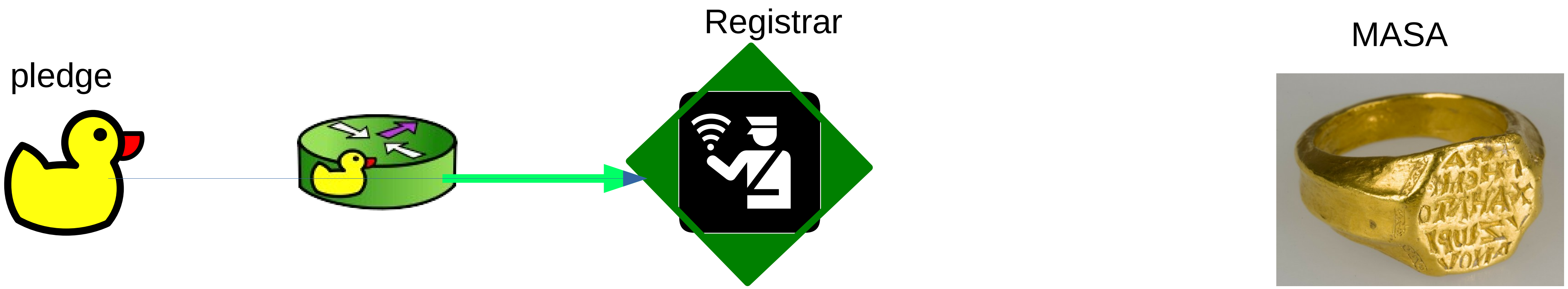
Discussed options for Registrar/MASA interaction
Use Same Format as received

pledge

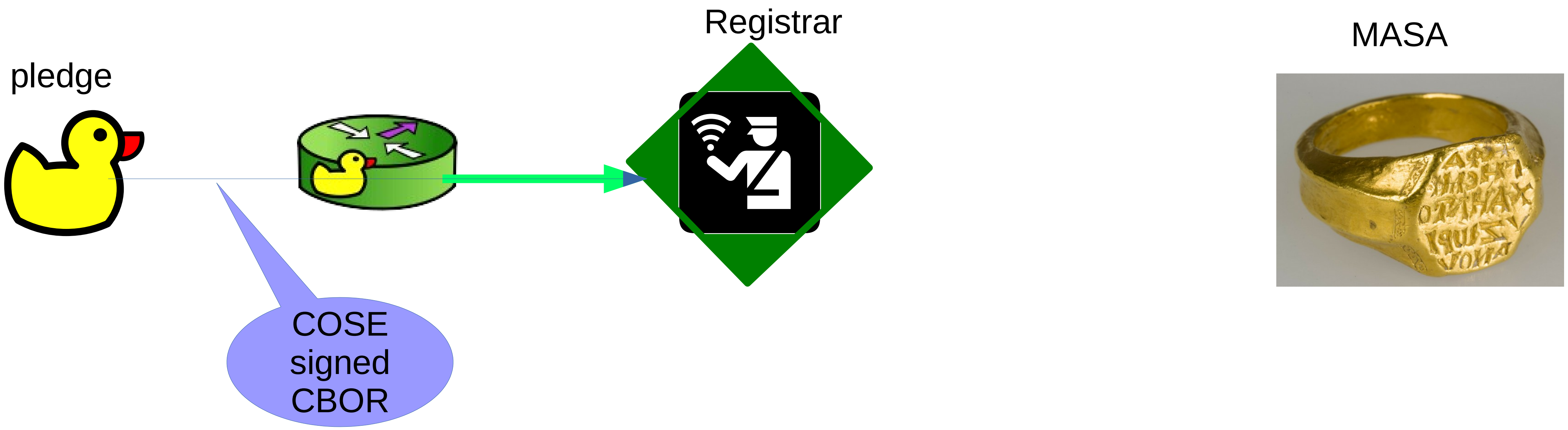
Registrar

MASA

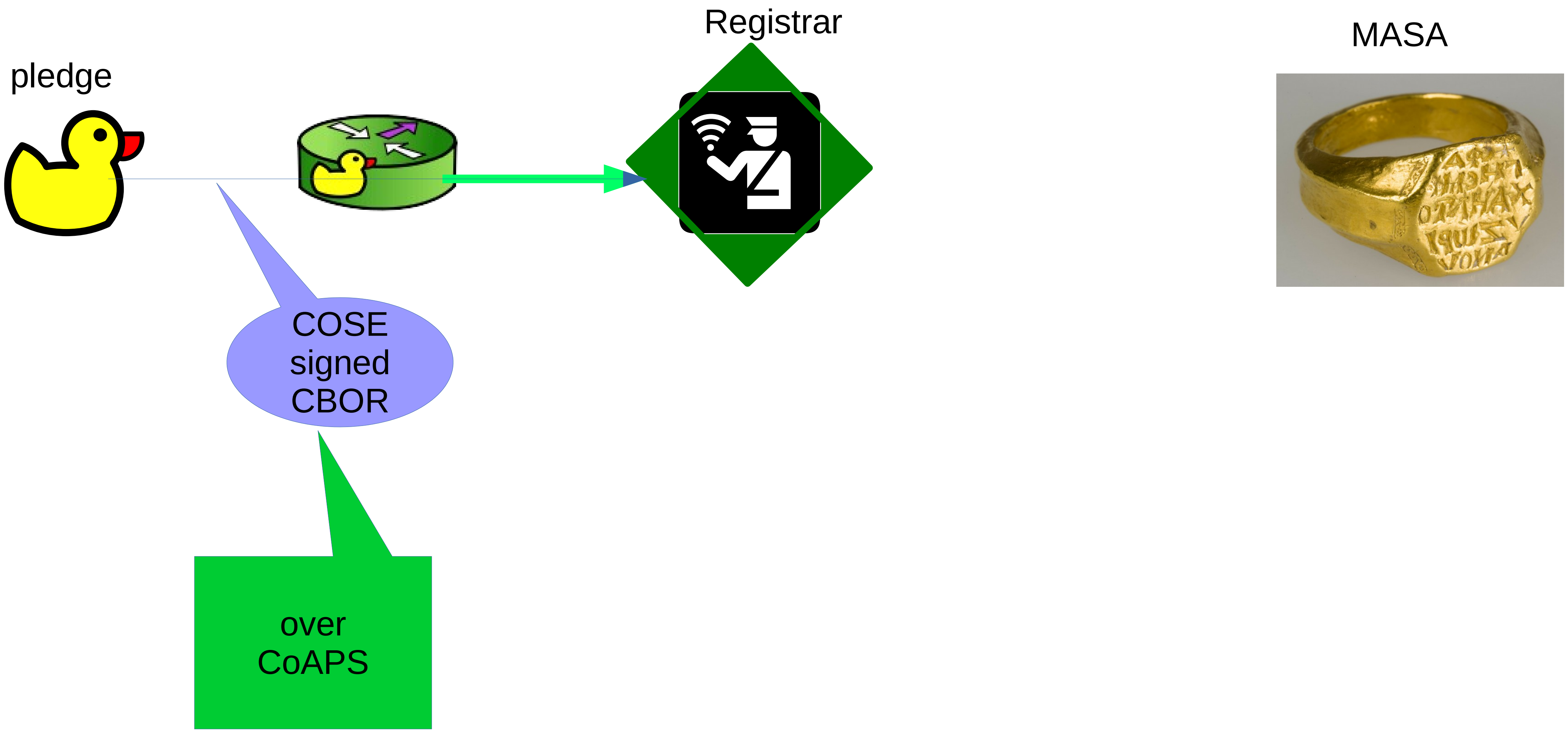
Discussed options for Registrar/MASA interaction
Use Same Format as received



Discussed options for Registrar/MASA interaction
Use Same Format as received



Discussed options for Registrar/MASA interaction
Use Same Format as received



pledge

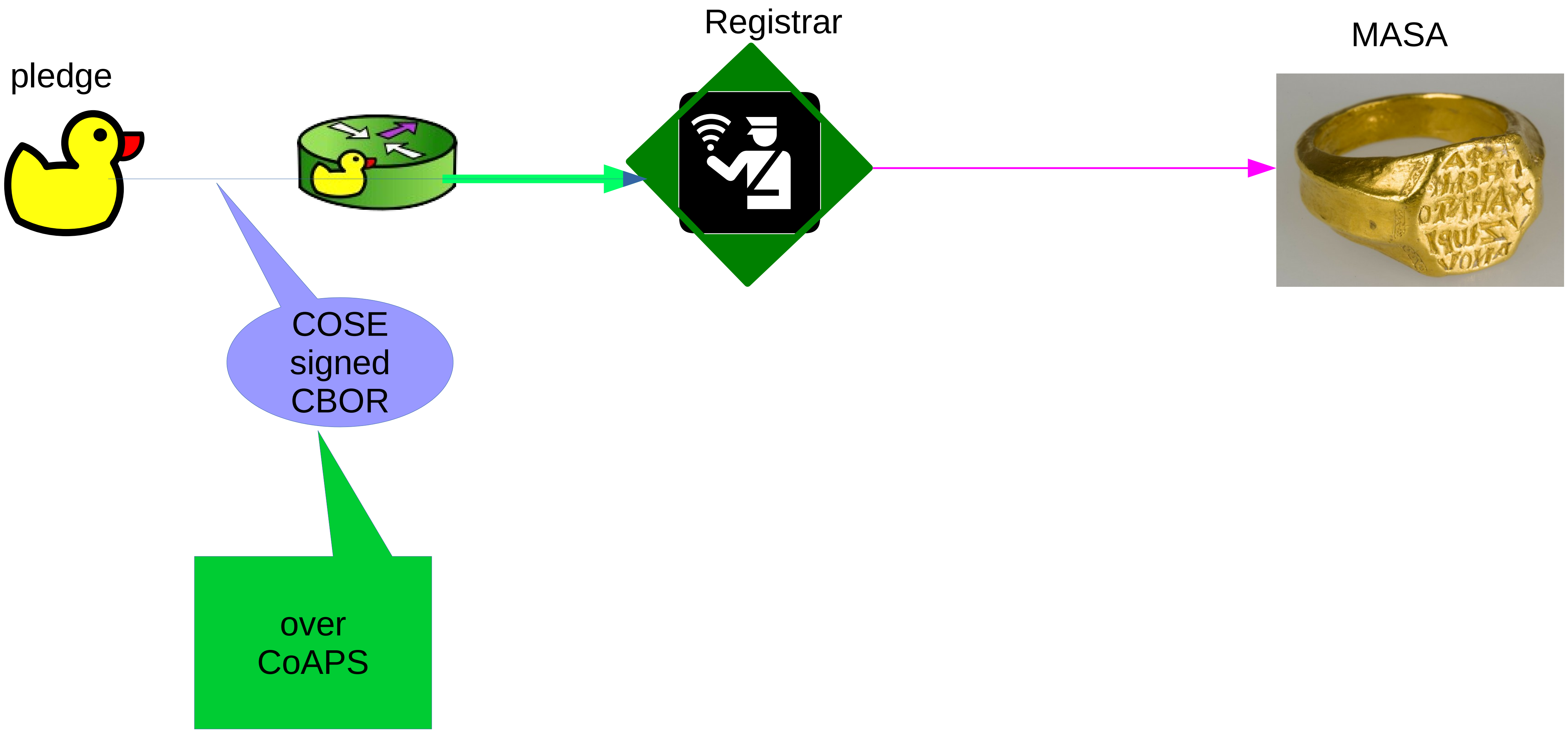
Registrar

MASA

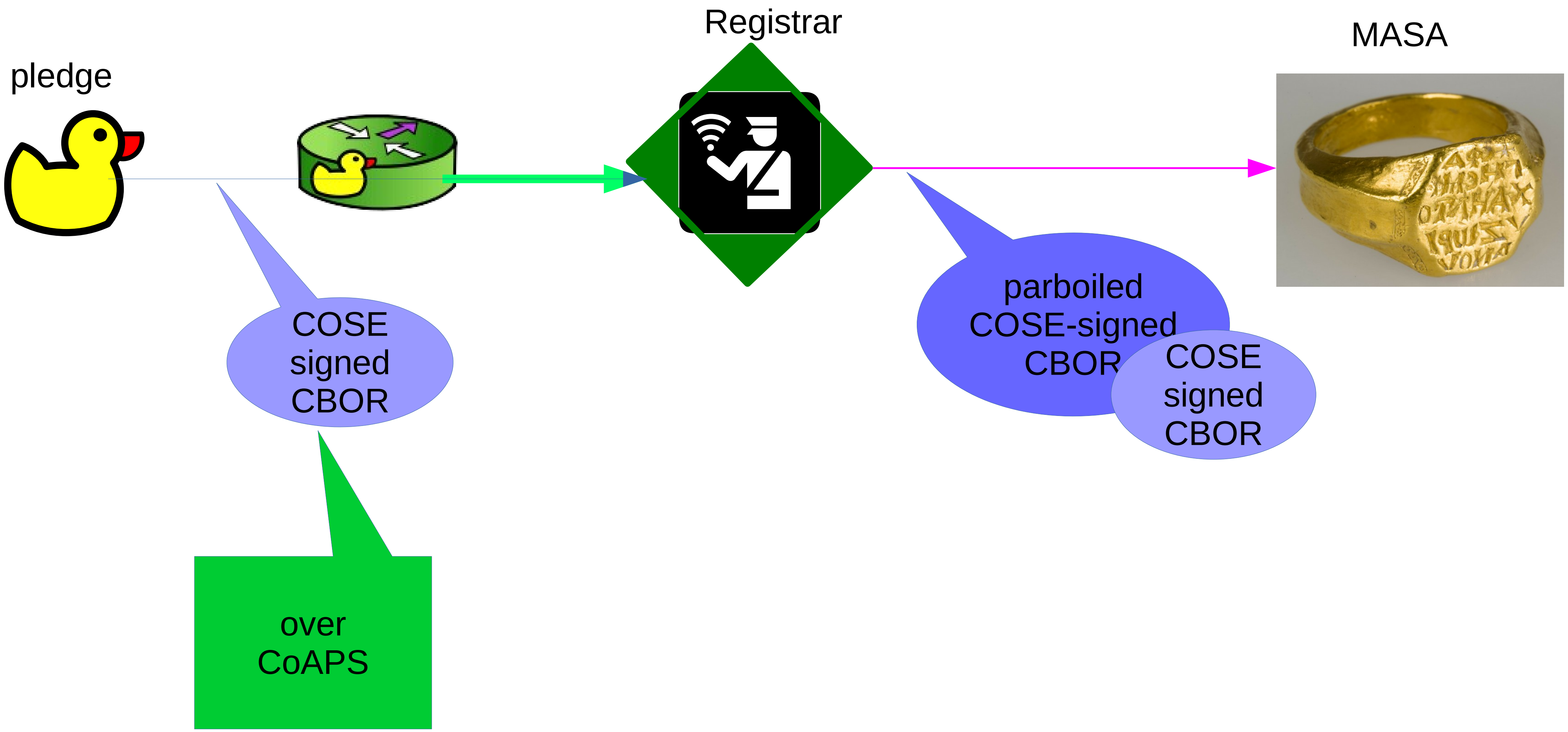
COSE signed CBOR

over CoAPS

Discussed options for Registrar/MASA interaction
Use Same Format as received



Discussed options for Registrar/MASA interaction
Use Same Format as received



pledge

Registrar

MASA

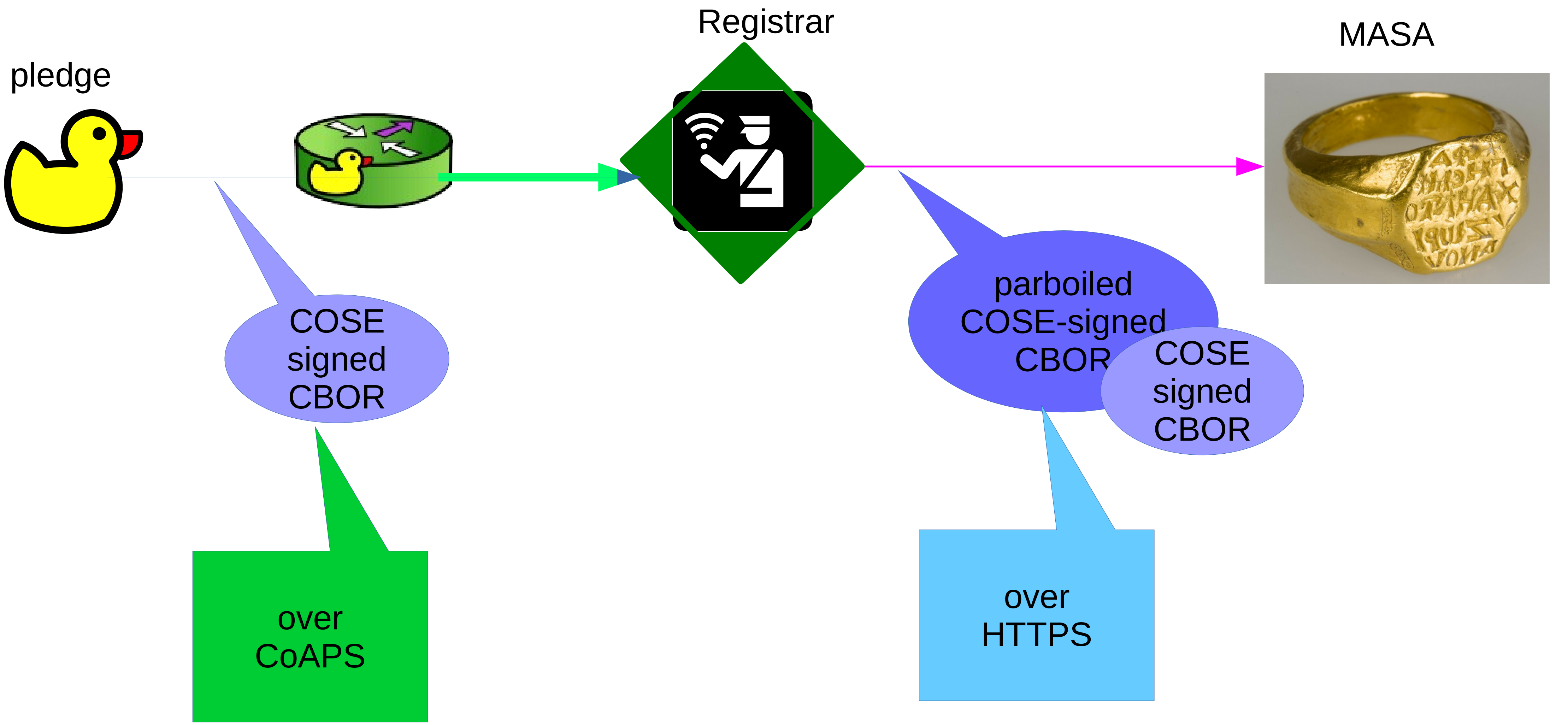
COSE signed CBOR

over CoAPS

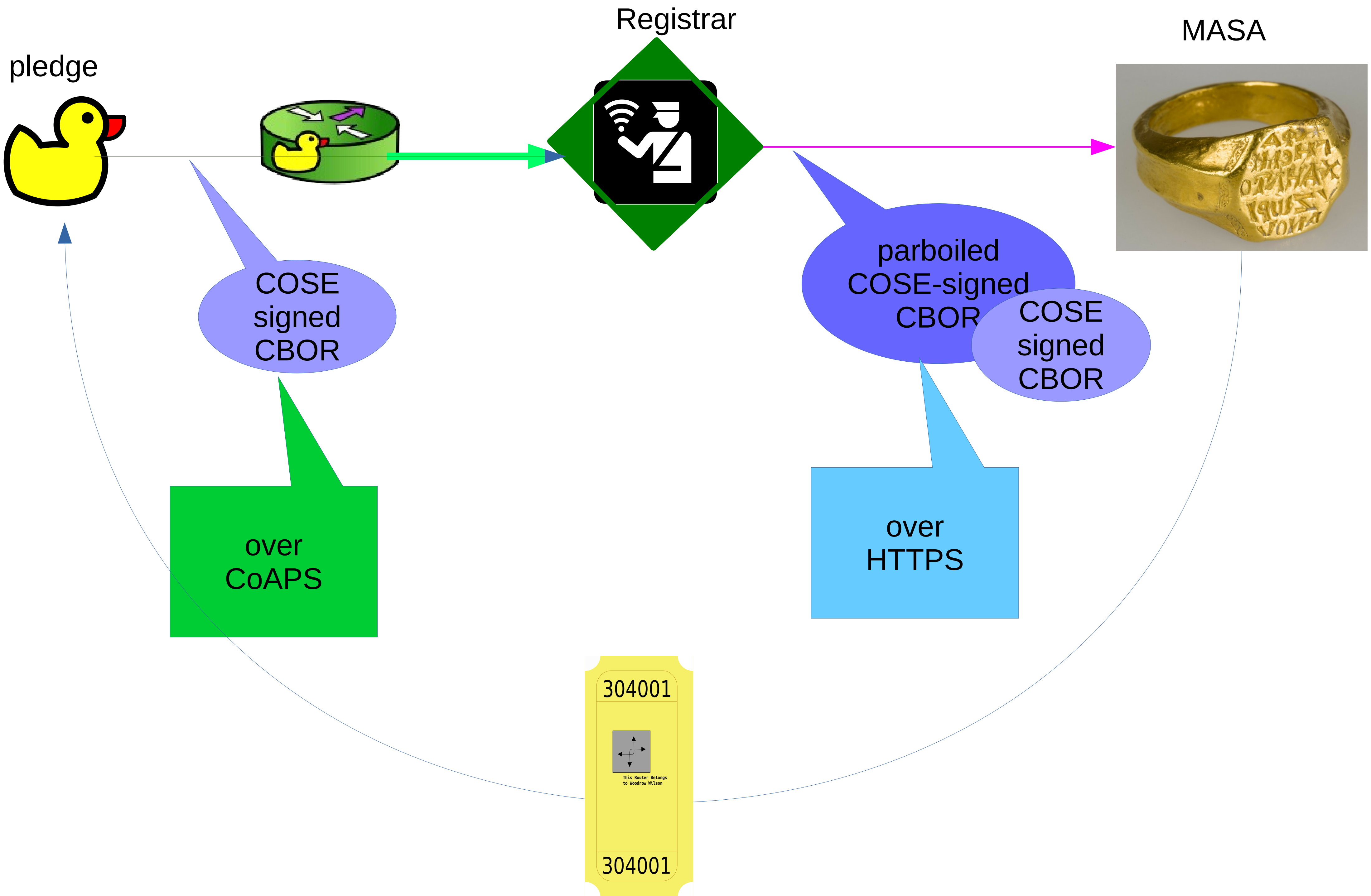
parboiled COSE-signed CBOR

COSE signed CBOR

Discussed options for Registrar/MASA interaction
Use Same Format as received



Discussed options for Registrar/MASA interaction
Use Same Format as received



pledge

Registrar

MASA

COSE signed CBOR

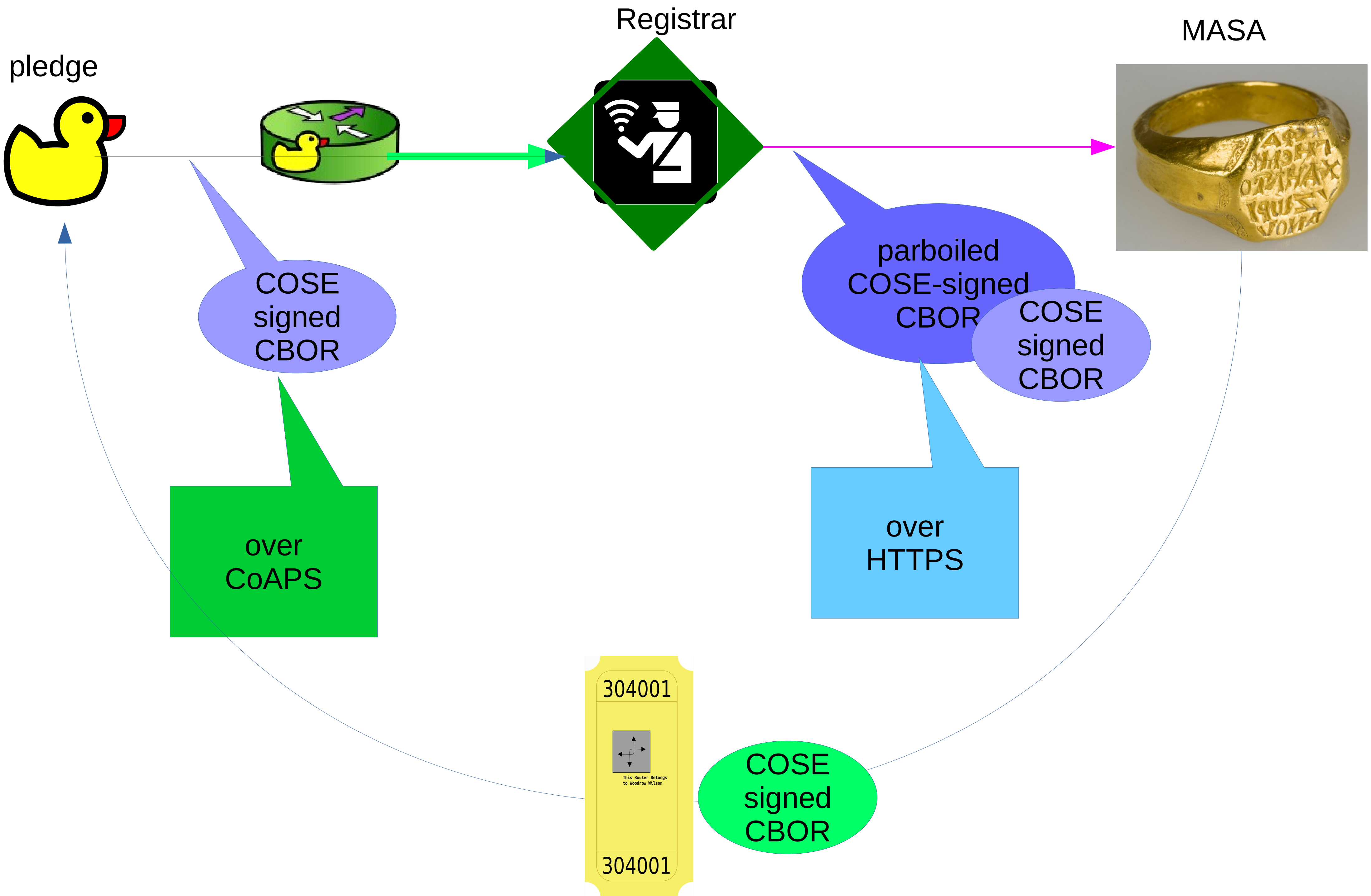
parboiled COSE-signed CBOR

COSE signed CBOR

over CoAPS

over HTTPS

Discussed options for Registrar/MASA interaction
Use Same Format as received



pledge

Registrar

MASA

COSE signed CBOR

over CoAPS

parboiled COSE-signed CBOR

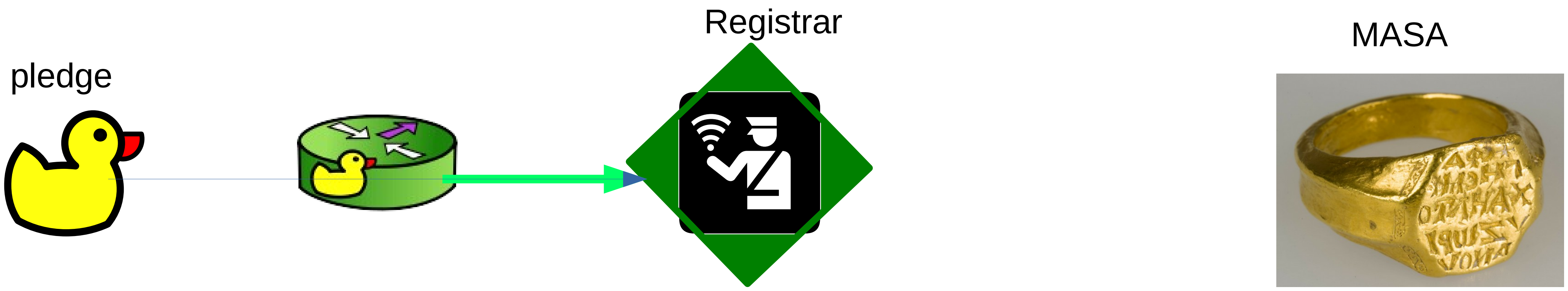
COSE signed CBOR

over HTTPS

COSE signed CBOR

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON

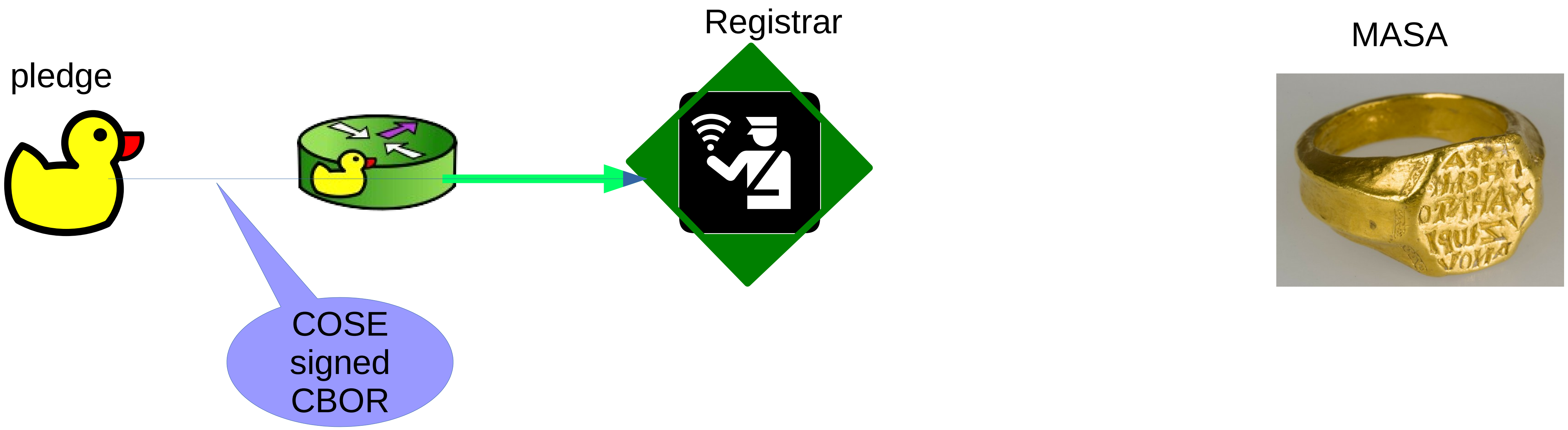


pledge

Registrar

MASA

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON



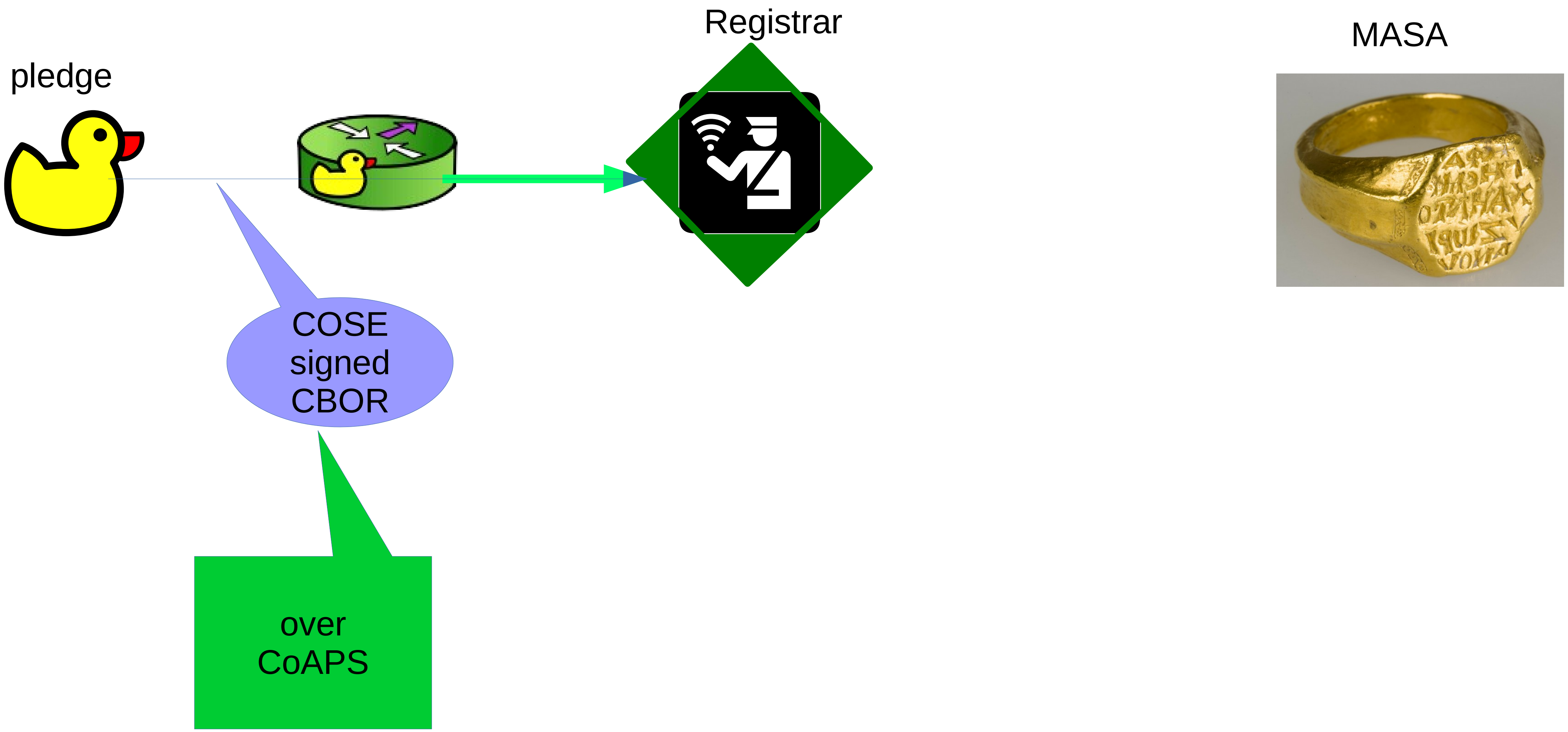
pledge

Registrar

MASA

COSE signed CBOR

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON



pledge

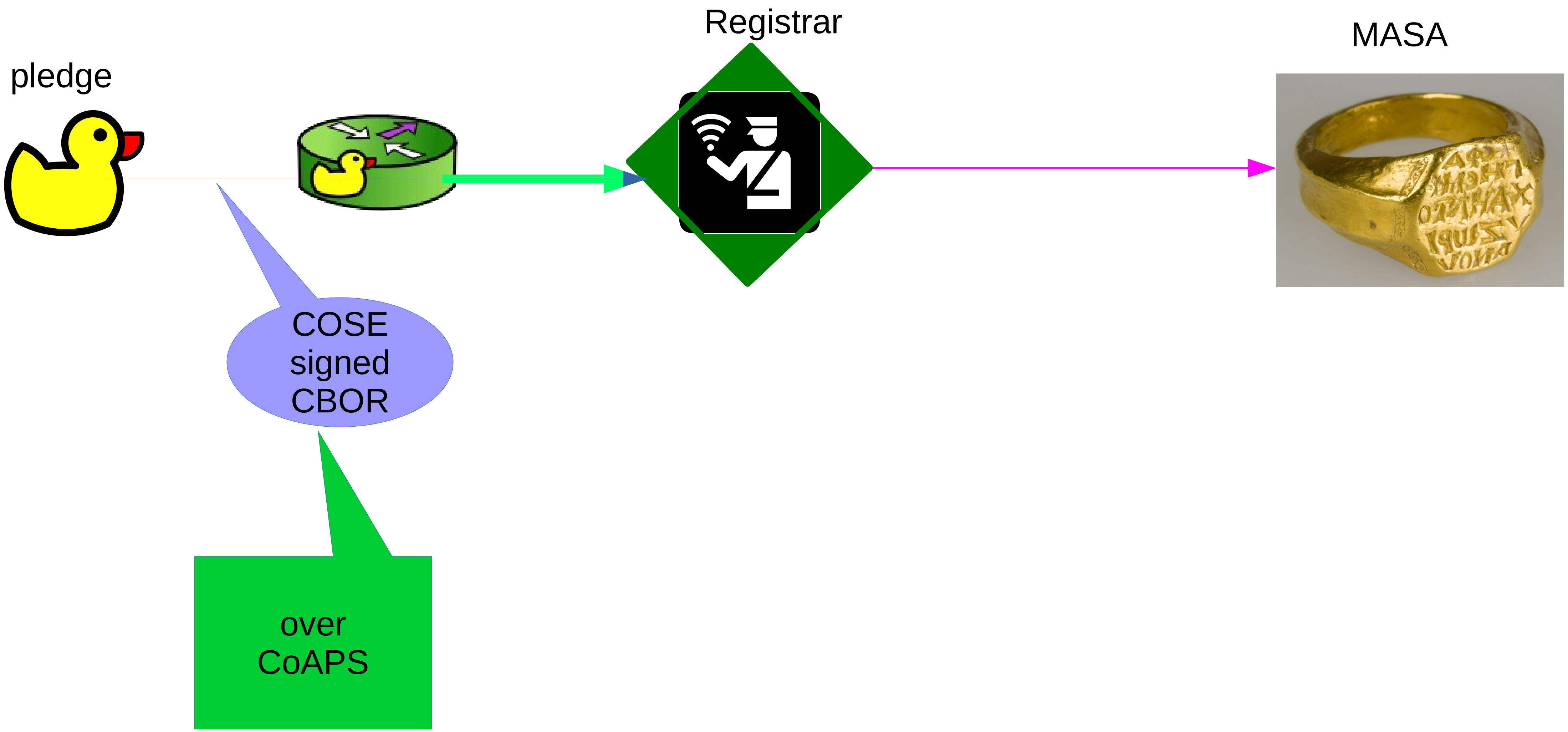
Registrar

MASA

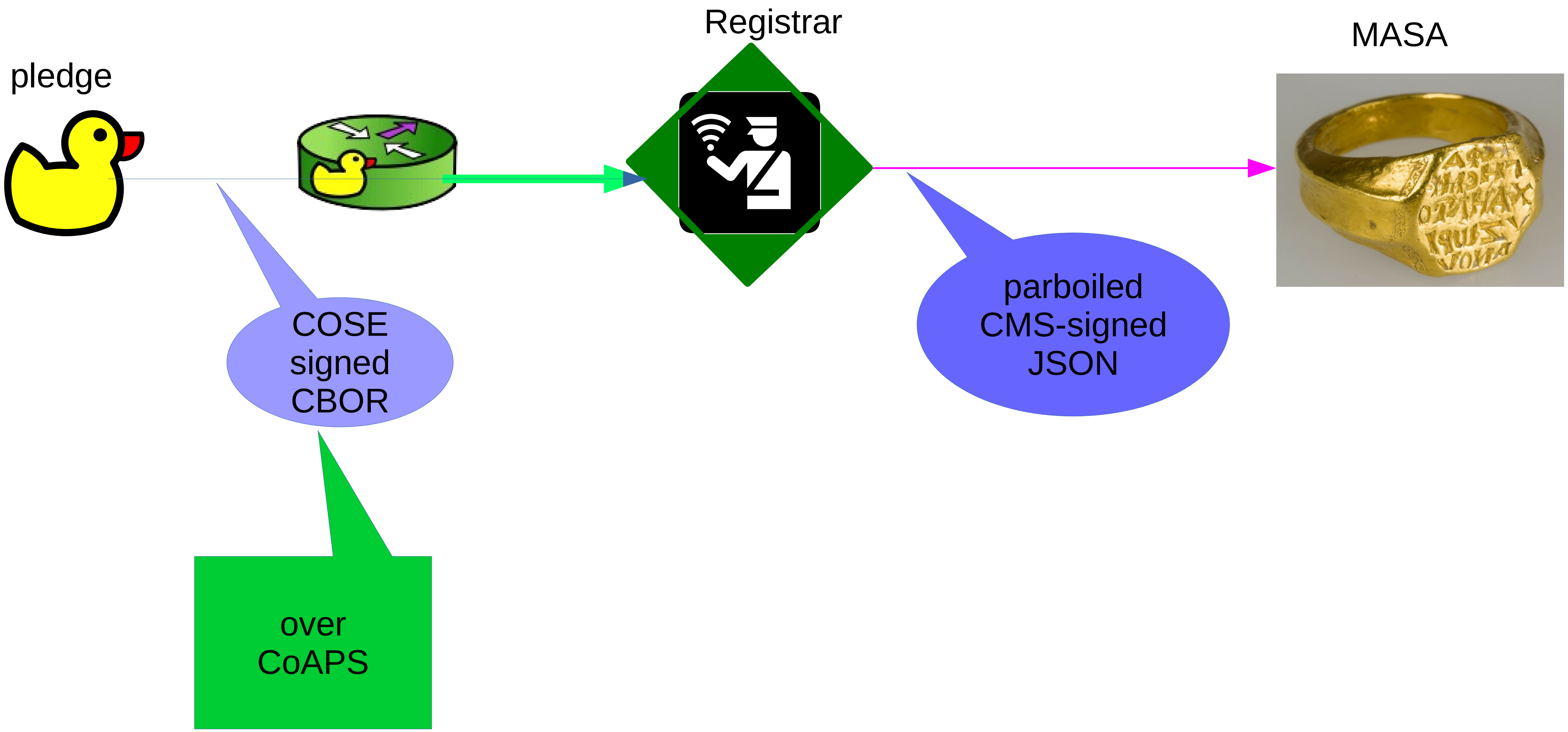
COSE signed CBOR

over CoAPS

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON



Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON



pledge

Registrar

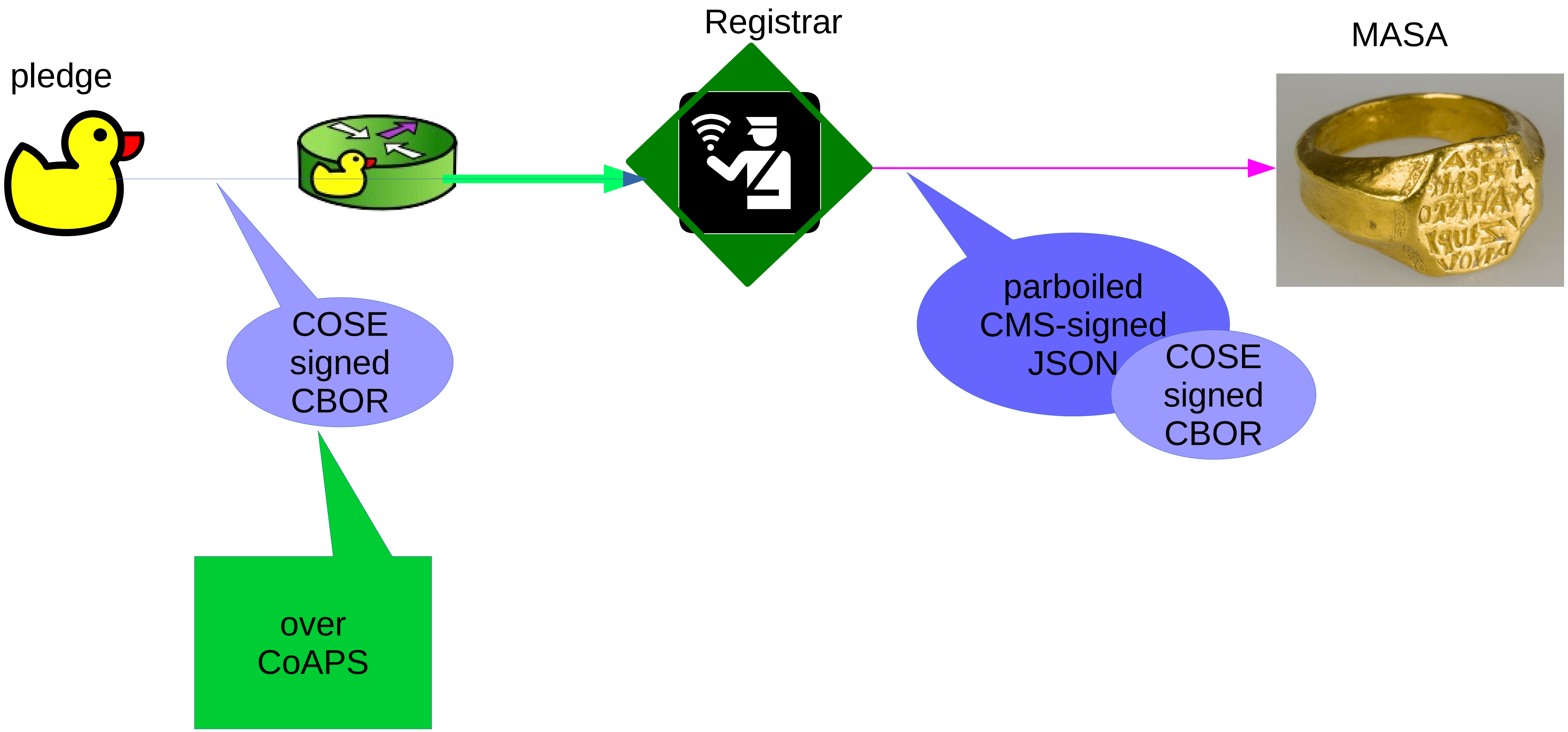
MASA

COSE signed CBOR

parboiled CMS-signed JSON

over CoAPS

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON



pledge

Registrar

MASA

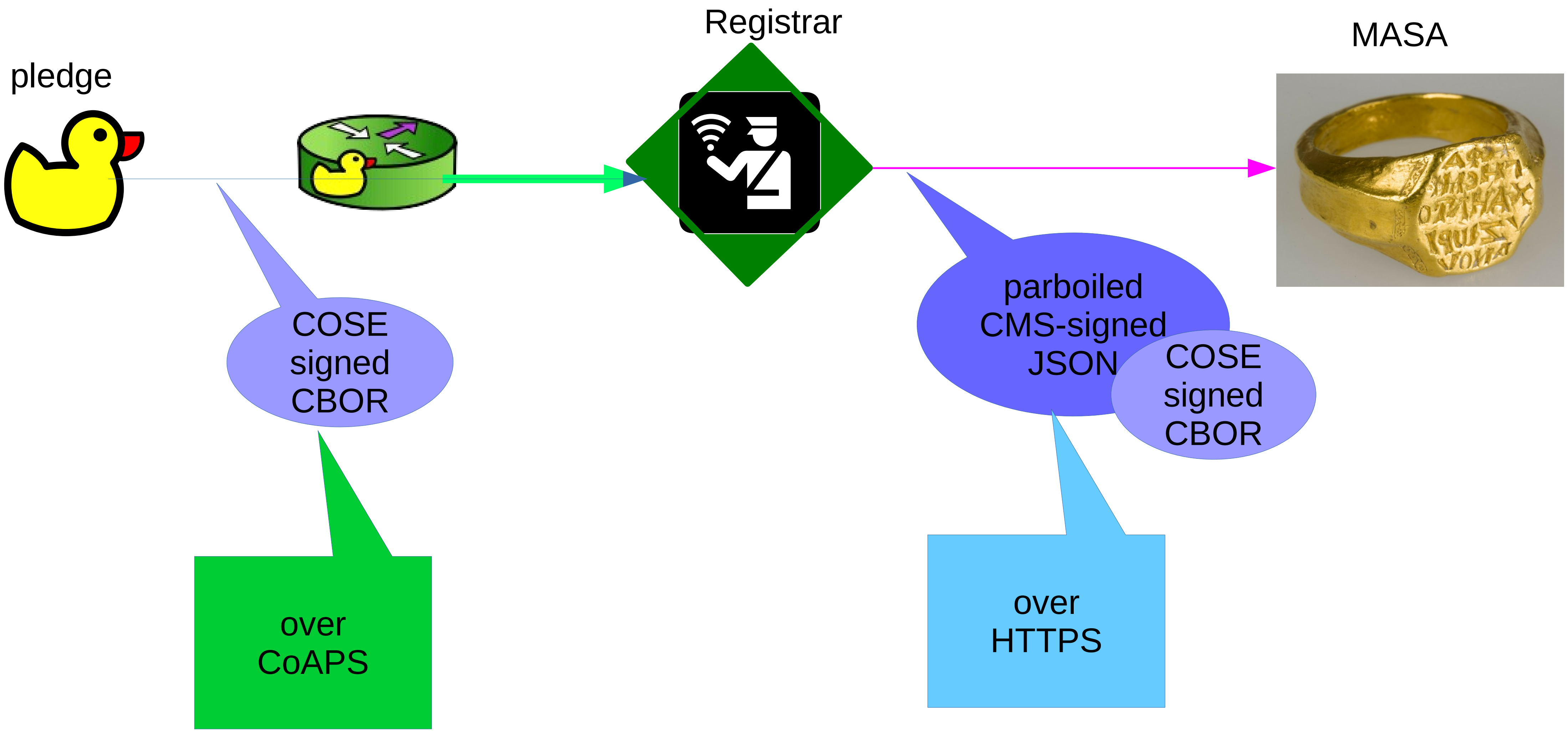
COSE signed CBOR

over CoAPS

parboiled CMS-signed JSON

COSE signed CBOR

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON



pledge

Registrar

MASA

COSE
signed
CBOR

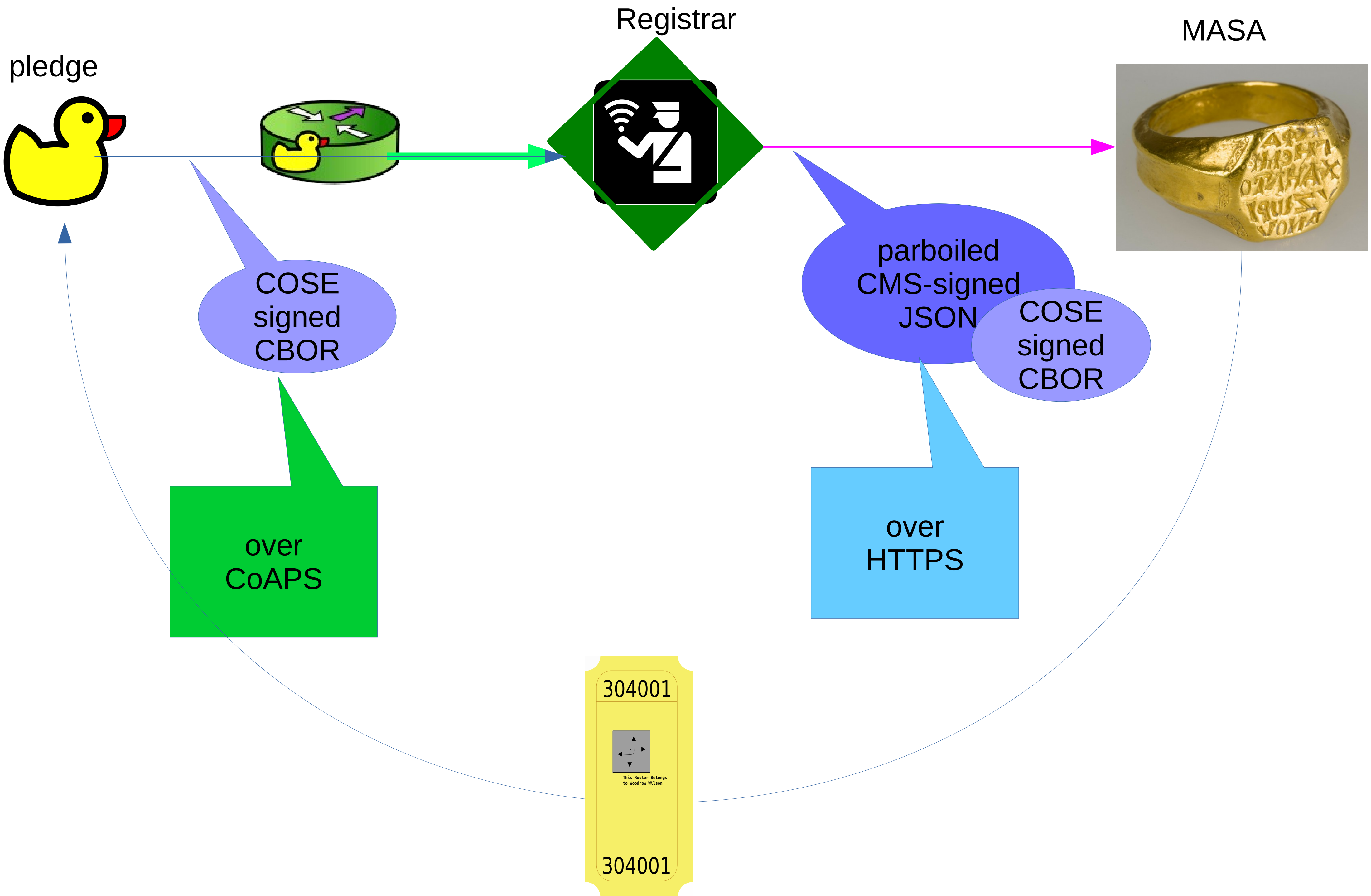
over
CoAPS

parboiled
CMS-signed
JSON

COSE
signed
CBOR

over
HTTPS

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON



pledge

Registrar

MASA

COSE signed CBOR

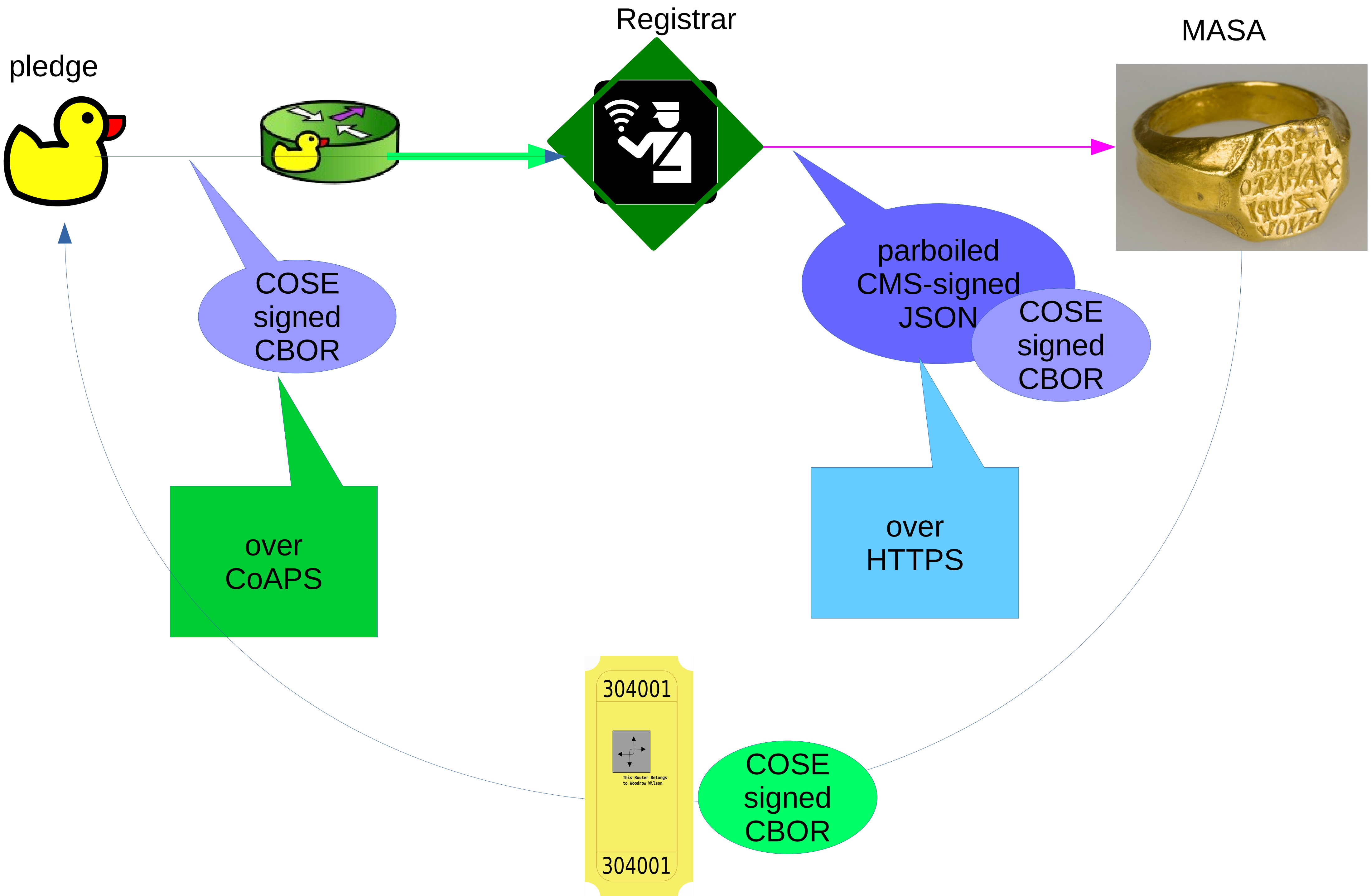
parboiled CMS-signed JSON

COSE signed CBOR

over CoAPS

over HTTPS

Discussed options for Registrar/MASA interaction
Always use CMS-signed-JSON



Registrar

MASA

pledge

COSE signed CBOR

over CoAPS

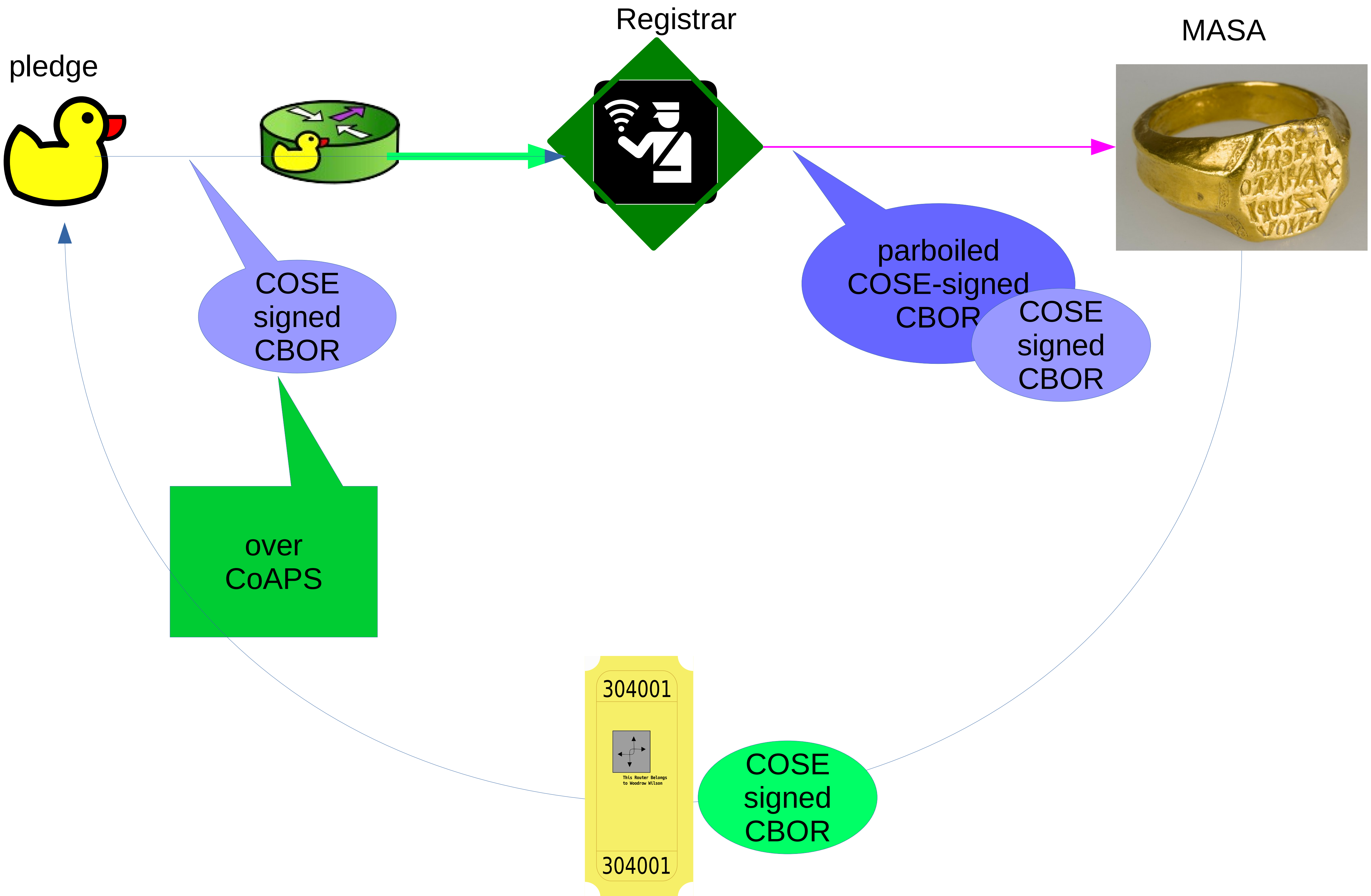
parboiled CMS-signed JSON

COSE signed CBOR

over HTTPS

COSE signed CBOR

Discussed options for Registrar/MASA interaction
Use CoAPS to MASA



pledge

Registrar

MASA

COSE signed CBOR

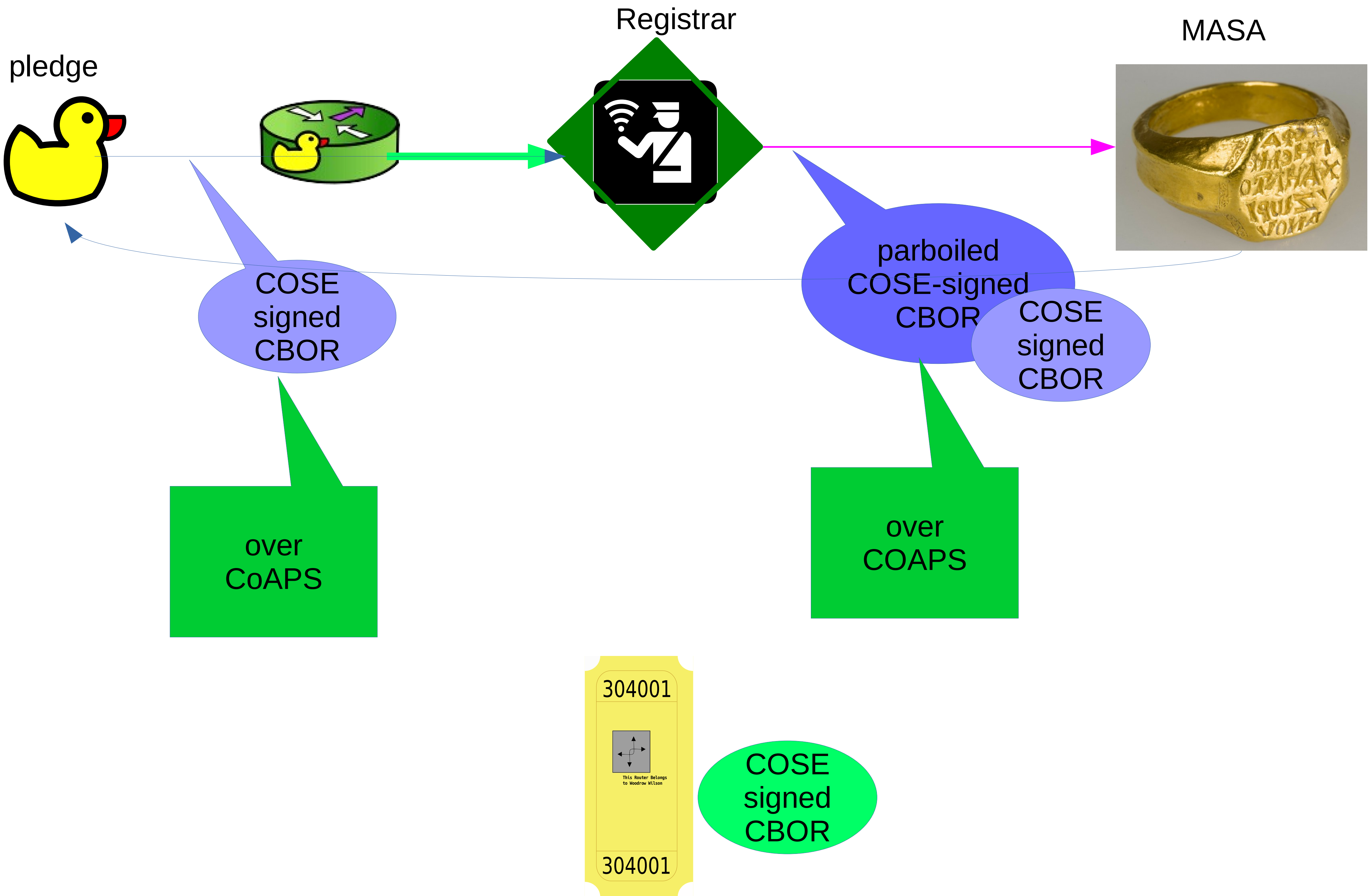
over CoAPS

parboiled COSE-signed CBOR

COSE signed CBOR

COSE signed CBOR

Discussed options for Registrar/MASA interaction
Use CoAPS to MASA



pledge

Registrar

MASA

COSE signed CBOR

over CoAPS

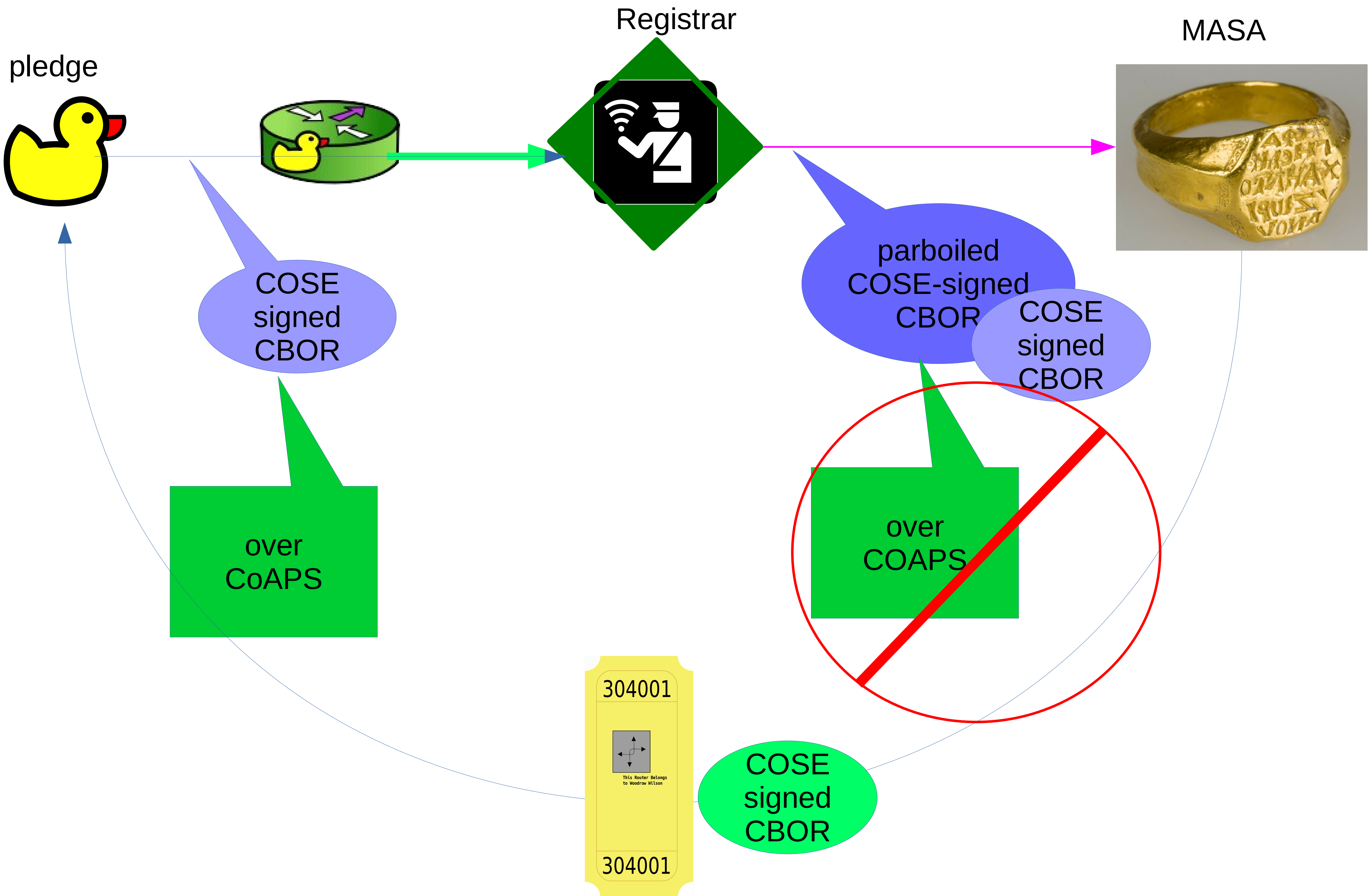
parboiled COSE-signed CBOR

COSE signed CBOR

over COAPS

COSE signed CBOR

Discussed options for Registrar/MASA interaction
Use CoAPS to MASA



pledge

Registrar

MASA

COSE signed CBOR

over CoAPS

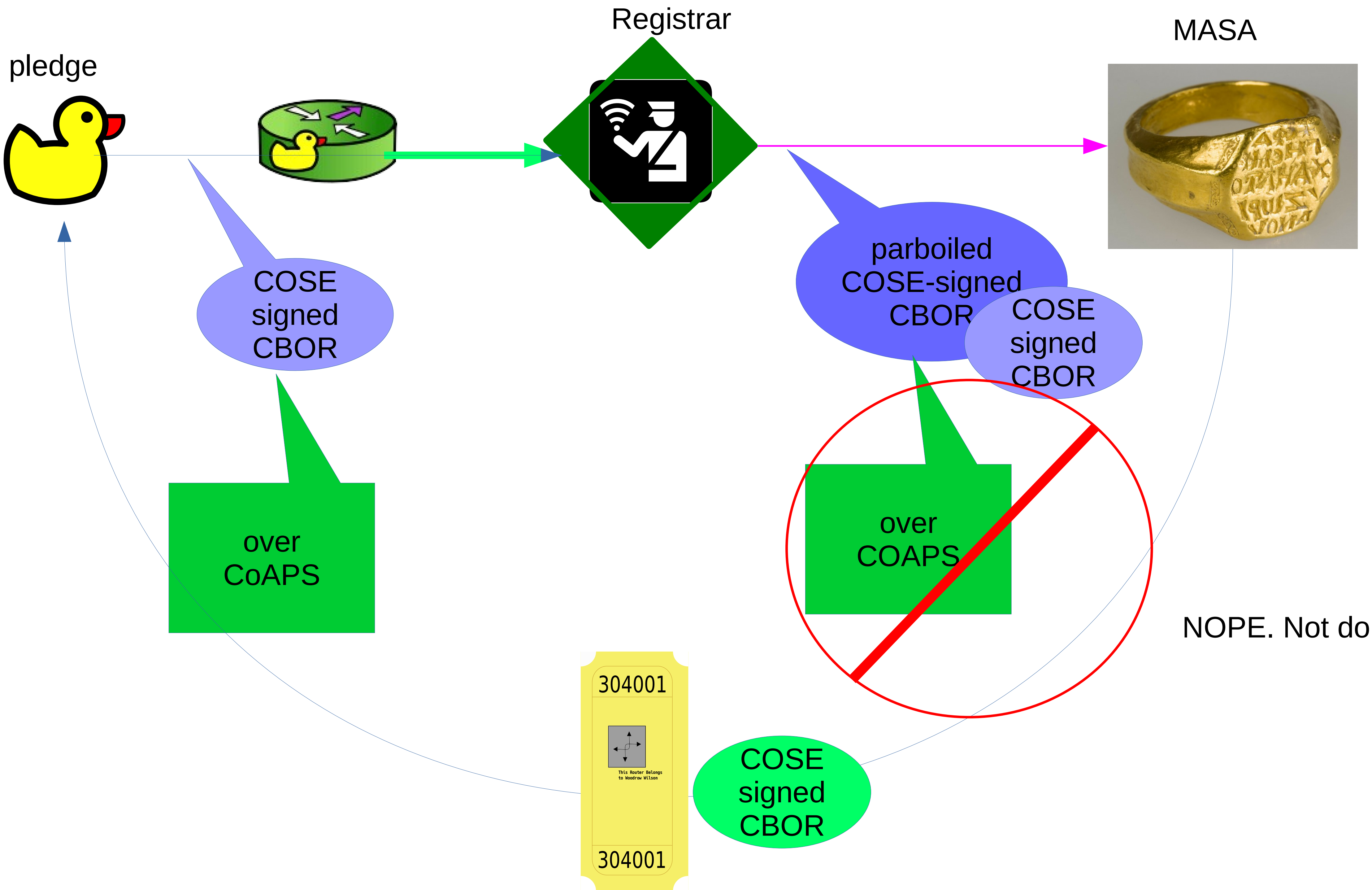
parboiled COSE-signed CBOR

COSE signed CBOR

over COAPS

COSE signed CBOR

Discussed options for Registrar/MASA interaction
Use CoAPS to MASA



pledge

Registrar

MASA

COSE signed CBOR

over CoAPS

parboiled COSE-signed CBOR

COSE signed CBOR

over COAPS

304001

This Router Belongs to Woodrow Wilson

304001

COSE signed CBOR

NOPE. Not doing this.

Registrar/MASA communication option breakdown

COSE-signed-CBOR

1) Registrar has to sign with COSE
2) MASA never needs to speak CMS, if pledge does not
3) Format of Voucher determined by Accept: header, and MASA knowledge of what pledge supports.

CMS-signed-JSON

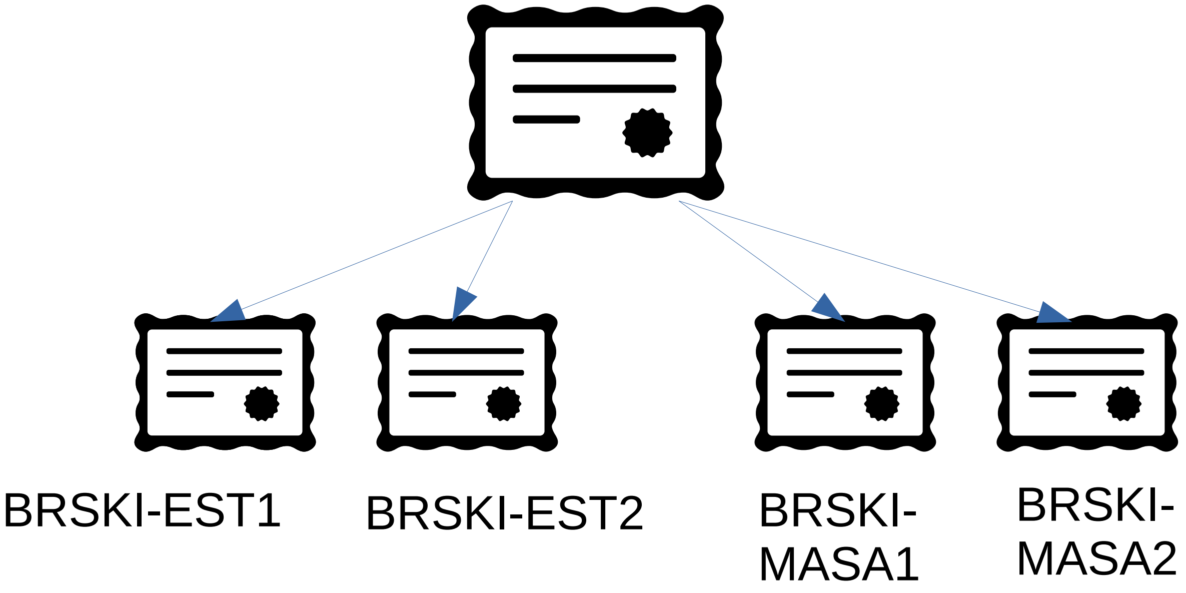
1) Registrar always just uses CMS
2) MASA has to speak CMS, even if pledge does not
3) JSON prior-signed-voucher-request contains COSE, not CMS. May need another attribute

Use CoAPS

1) Registrar uses same protocl it receives.
2) Likely challenges for CoAP to leave Enterprise/Corporate environment.
3) No industry experience scaling CoAP based systems (vs HTTPS based, which is ubiquitous)
4) no relation to content, but assumed that CMS would never be used

Challenges with Asynchronous Registrar and pinning of public key

- In Asynchronous Registrar situation, the Southbound Pledge Interface has possibly many instances, each with it’s own certificate/public key.
- The pledge will pin the public key that it sees as the `pinned-domain-subject-public-key-info.` This is **just** the public key, and contains no certificate chain information.
- In simple/synchronous Registrar, the parboiled voucher-request would get signed by the same key pair as is pinned by the pledge. The MASA would therefore be able to see an entire certificate chain (from the x5u COSE pair, see draft-ietf-cose-x509-06 section 2), and would know who the registrar is.
  - (it would still put the required public key into the voucher)
- In the asynchronous registrar situation, then the relationship is not obvious, so the Registrar MUST include additional certificates leading to a common Root Certificate.



```
                  .------------.
                  |    MASA    |
                  |   client   |
                  | BRSKI-MASA |
                  '------------'
                         ^
                         |
 .------------.          |           .---------------.
 | management |    .----------.      | certification |
 | interface  |<---| database |----->|   authority   |
 '------------'    '----------'      '---------------'
                         |
                         |
                         v
.------------.     .-----------.       .------------.
| Join Proxy |     |  Pledge   |--.    | EST/BRSKI  |
|------------|     | Interface |  |    |------------|
| GRASP      |     | BRSKI-EST |e |    |    GRASP   |
| (DULL)     |     '-----------'T |    '------------'
'------------'        '-----------'
```

Figure 1: Reference Internal Architecture for Registrar

from
draft-richardson-anima-registrar-considerations
section 1.3
and section 4.3 **Asynchronous Registrar**

Conclusion

Good progress since BRSKI document is ready for publication

Examples need to be consolidated

Additional explanatory text needed

Draft relations

Draft	WG	uses	extends
BRSKI	ANIMA	HTTP/TLS EST CMS	EST with Voucher requests MASA Circuit proxy
EST-coaps	ACE	CoAP/DTLS EST multipart-ct draft	EST with CoAP/DTLS
Voucher	ANIMA	YANG/JSON CMS	BRSKI with voucher spec
Constrained voucher	ANIMA	YANG/CBOR Voucher COSE/CMS/CBOR	Voucher with 2 fields BRSKI with COSE/CBOR and SID BRSKI with CMS/CBOR and SID
Constrained Join-proxy	ANIMA	CBOR multipart-ct draft	BRSKI with constrained join proxy and EST-coaps

Constrained join proxy

draft-vanderstok-anima-constrained-join-proxy-04

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 109

ANIMA Working Group

Constrained Join Proxy

BRSKI uses HTTP and TLS

This draft proposes
- Replacement of circuit proxy, using
- CoAP and DTLS to support connection between
  Pledge and Domain Registrar

Based on `kumar-dice-dtls-relay`

EST: Enrollment over Secure Transport (RFC7030)
BRSKI: Bootstrapping of Remote Secure Key Infrastructures

Current state

Two versions:

- Stateful one: currently implemented
  - (essentially NAPT)
- Stateless one:

    + needs some fine tuning

    + change to specification needed

Looking forward to WG adoption