Certification
RIPE NCC beta programme

Topics

- Driving forces
- Introduction of resource certification concepts
- What's in it for you?
- Demo of the beta application
- A look into the future
- Questions

Driving forces...

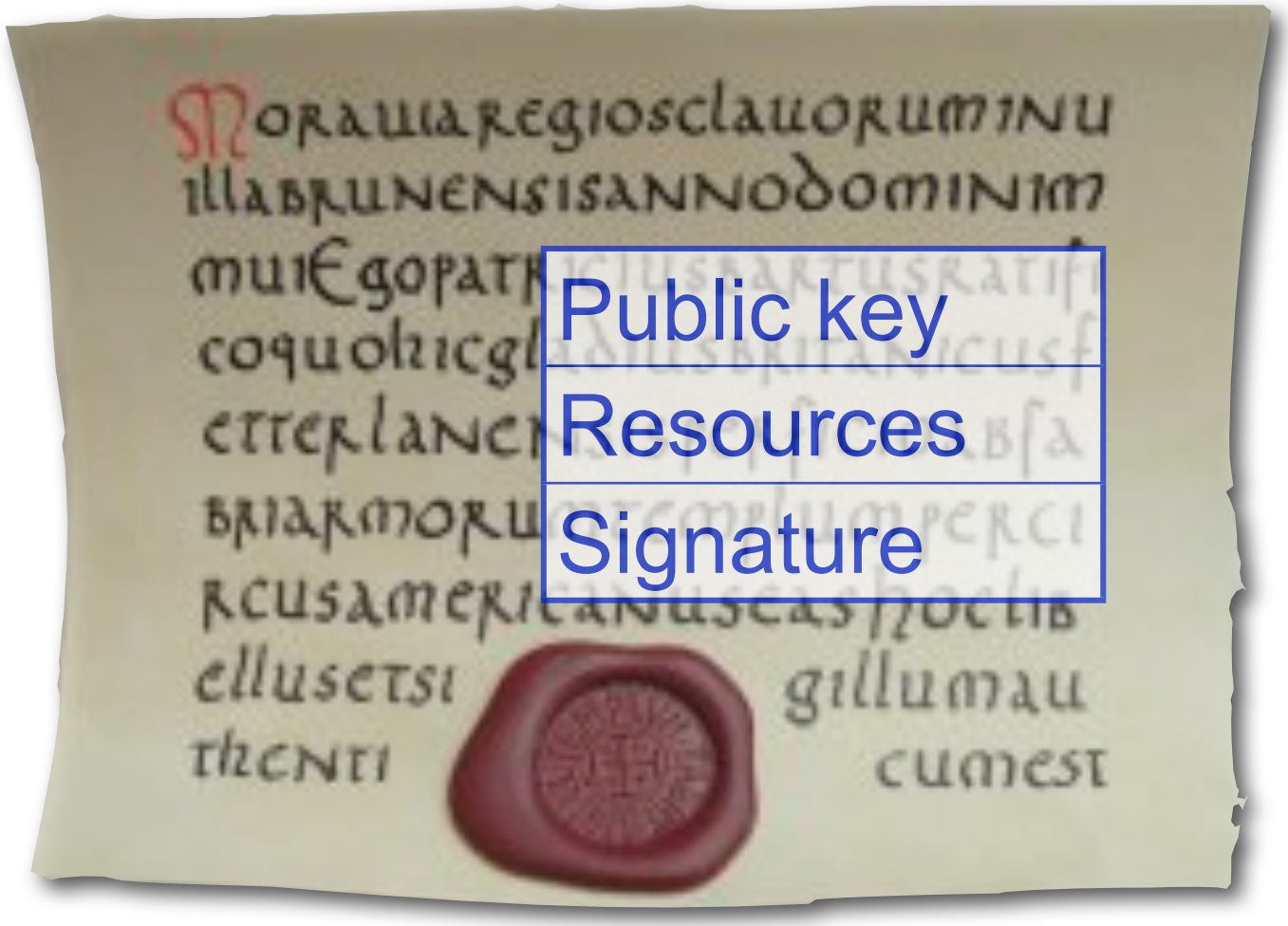
- IETF
  - Discussing ideas, finding consensus on global scale
  - Defining resource certification concepts
- RIPE
  - Certificate Authority Task Force (CA-TF)
    - Applying certification in the RIPE region
    - Policy proposals
    - RIPE NCC beta programme

Beta programme

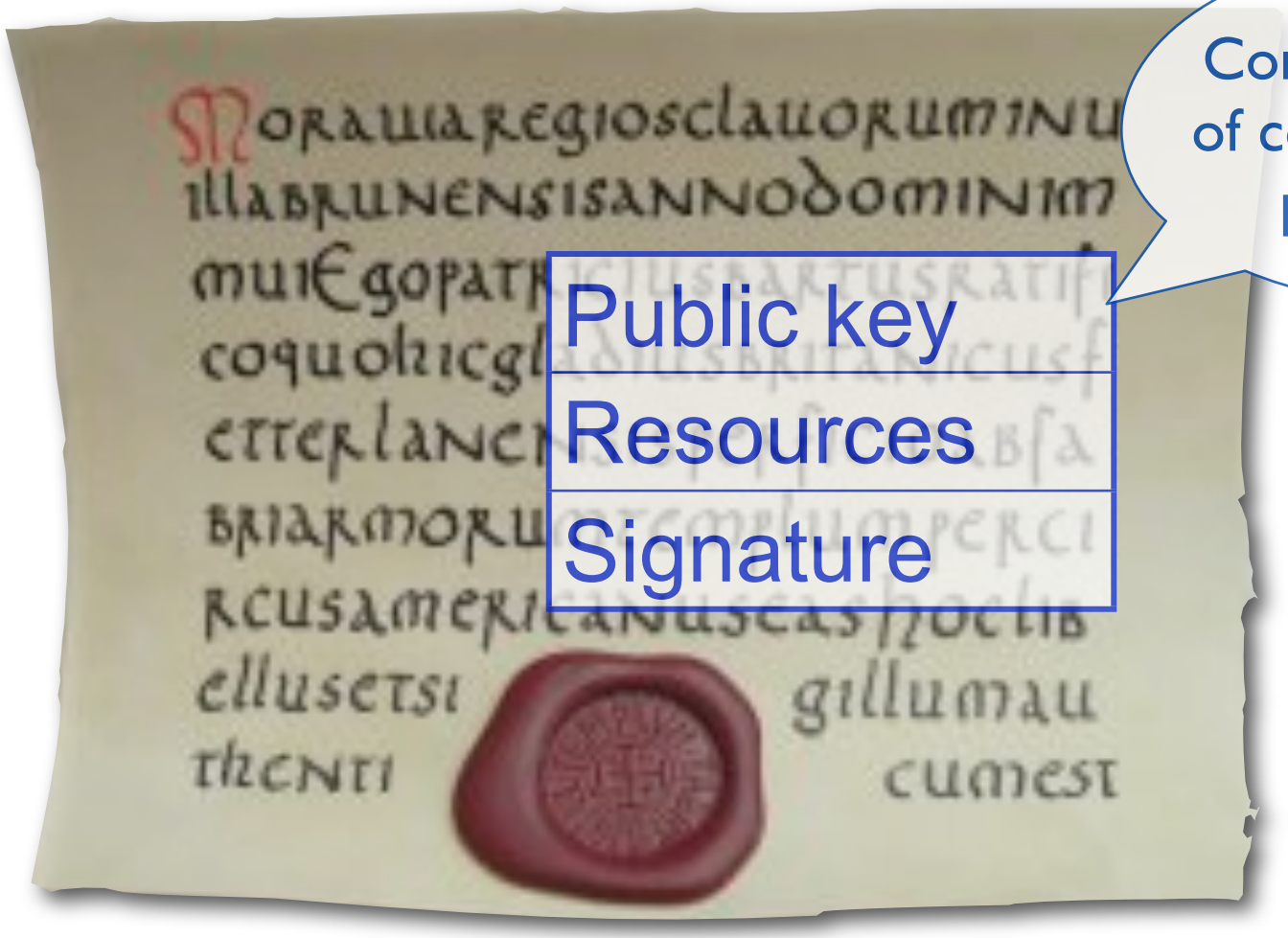
- Development started end of 2007 for CA-TF
- Focus on elements of resource certification where:
  - consensus has been reached in the IETF and CA-TF
  - immediate benefit for members is achieved

- Start simple
- Involve members from an early stage

Resource certificates

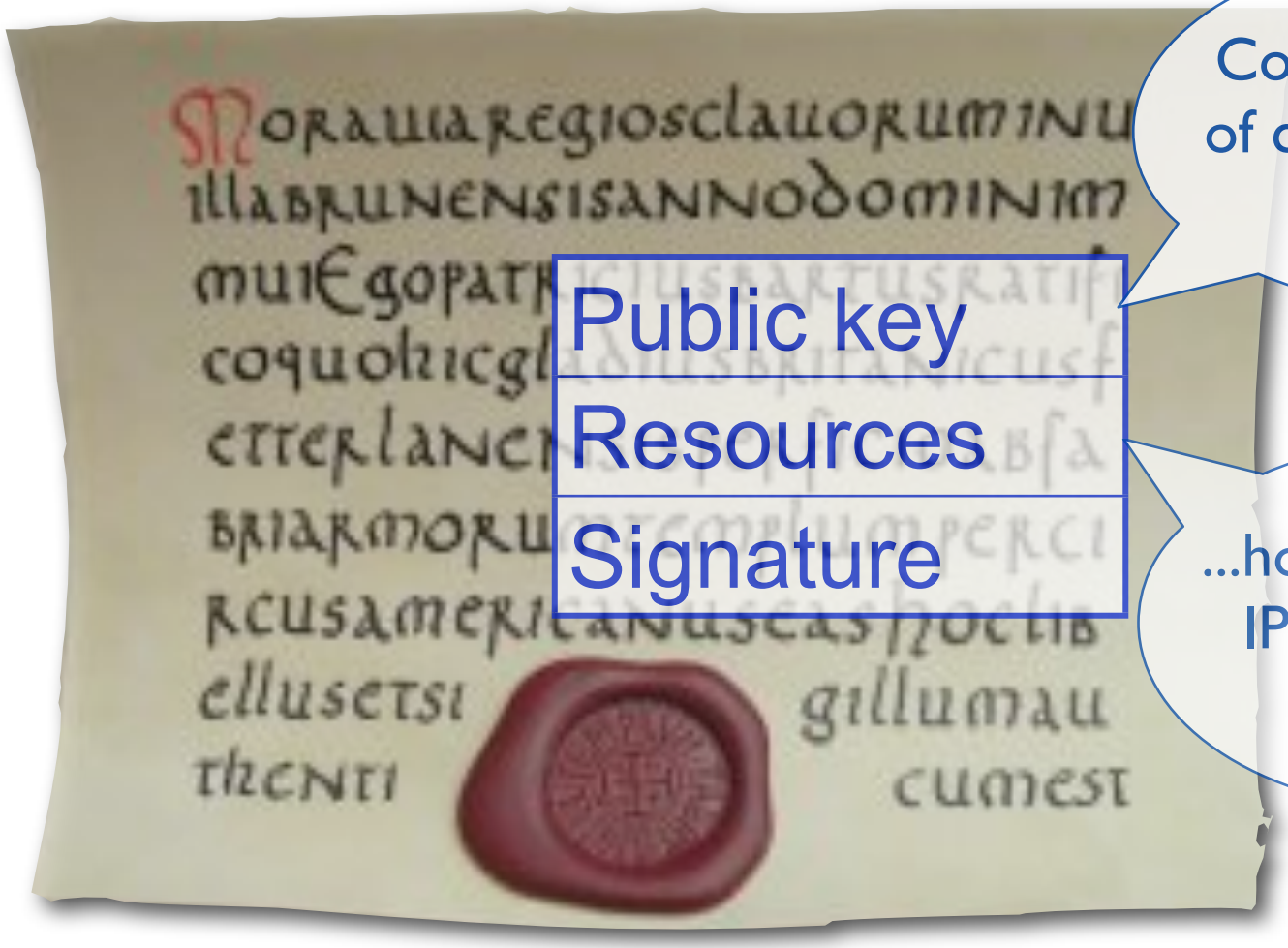


Resource certificates



Consider owner of corresponding private key...

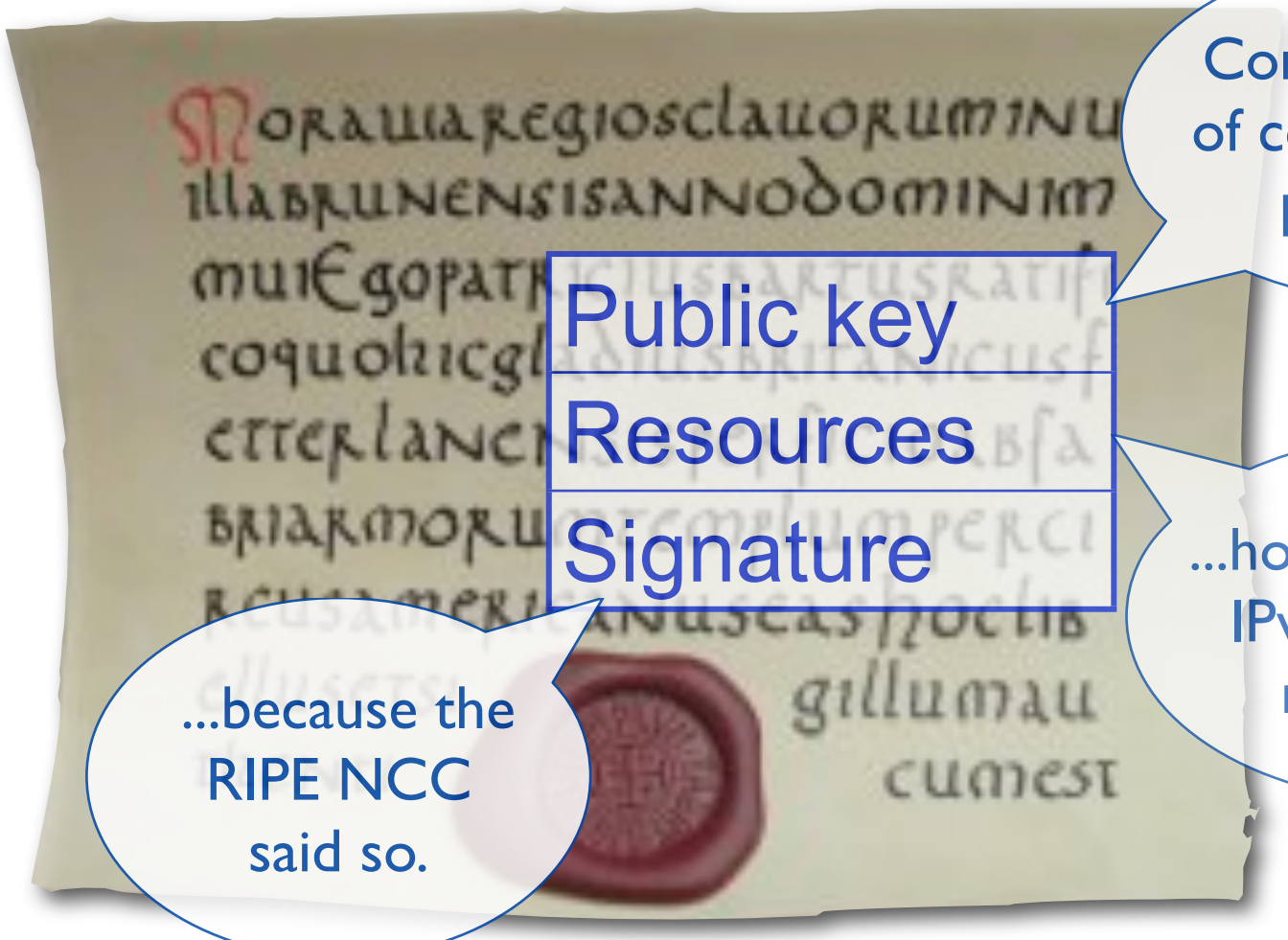
Resource certificates



Consider owner of corresponding private key...

...holder of named IPv4, IPv6, ASN resources...

Resource certificates



Public key

Resources

Signature

Consider owner of corresponding private key...

...holder of named IPv4, IPv6, ASN resources...

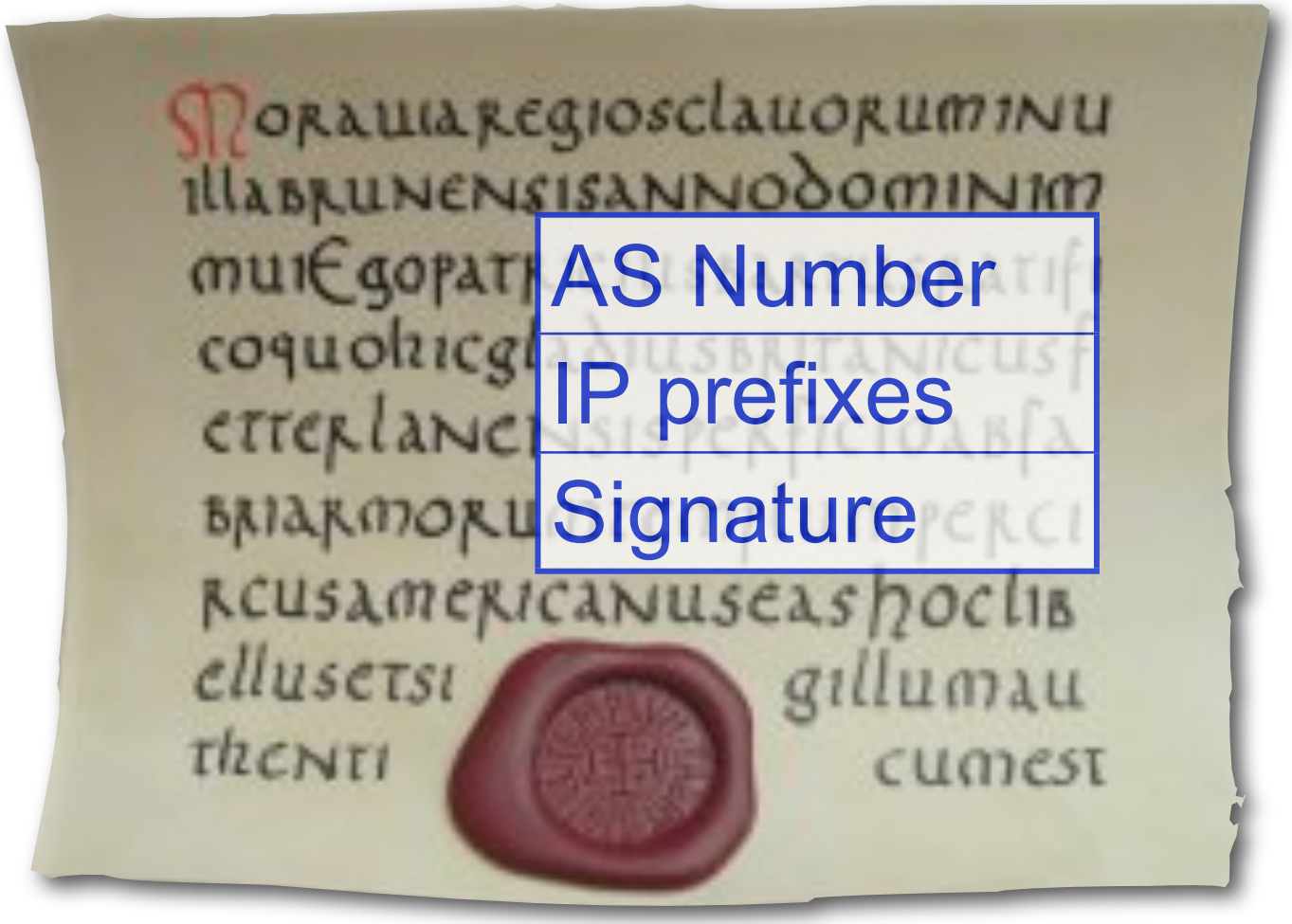
...because the RIPE NCC said so.

Resource certificates

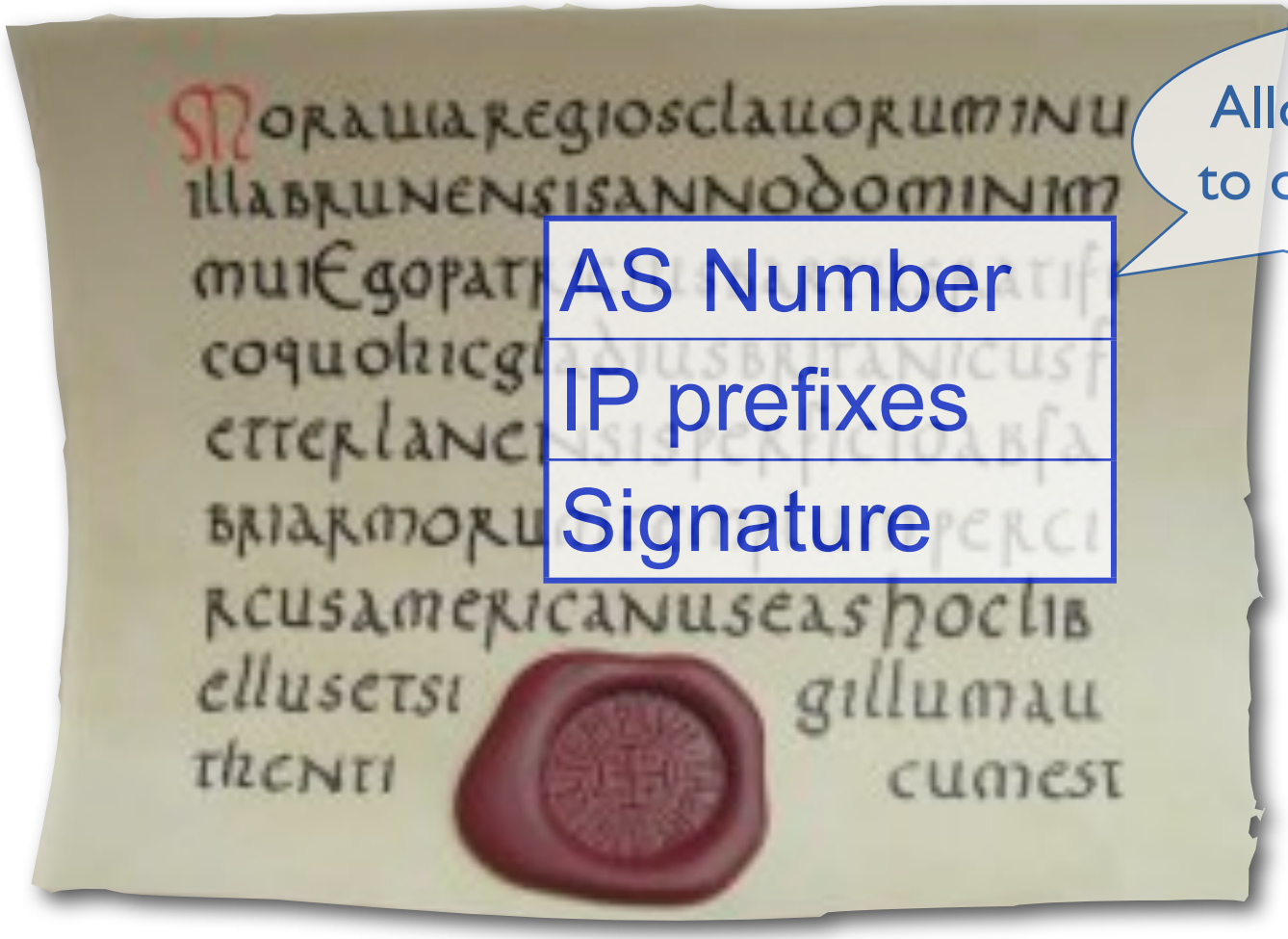
- Certificates contain public information only
- Certificates do *not* attest to the identity of the certificate holder.

- Holder of *private* key for certificate can *sign* specific objects.
- Relying parties can verify *proof of holdership* of resources mentioned on these signed objects.

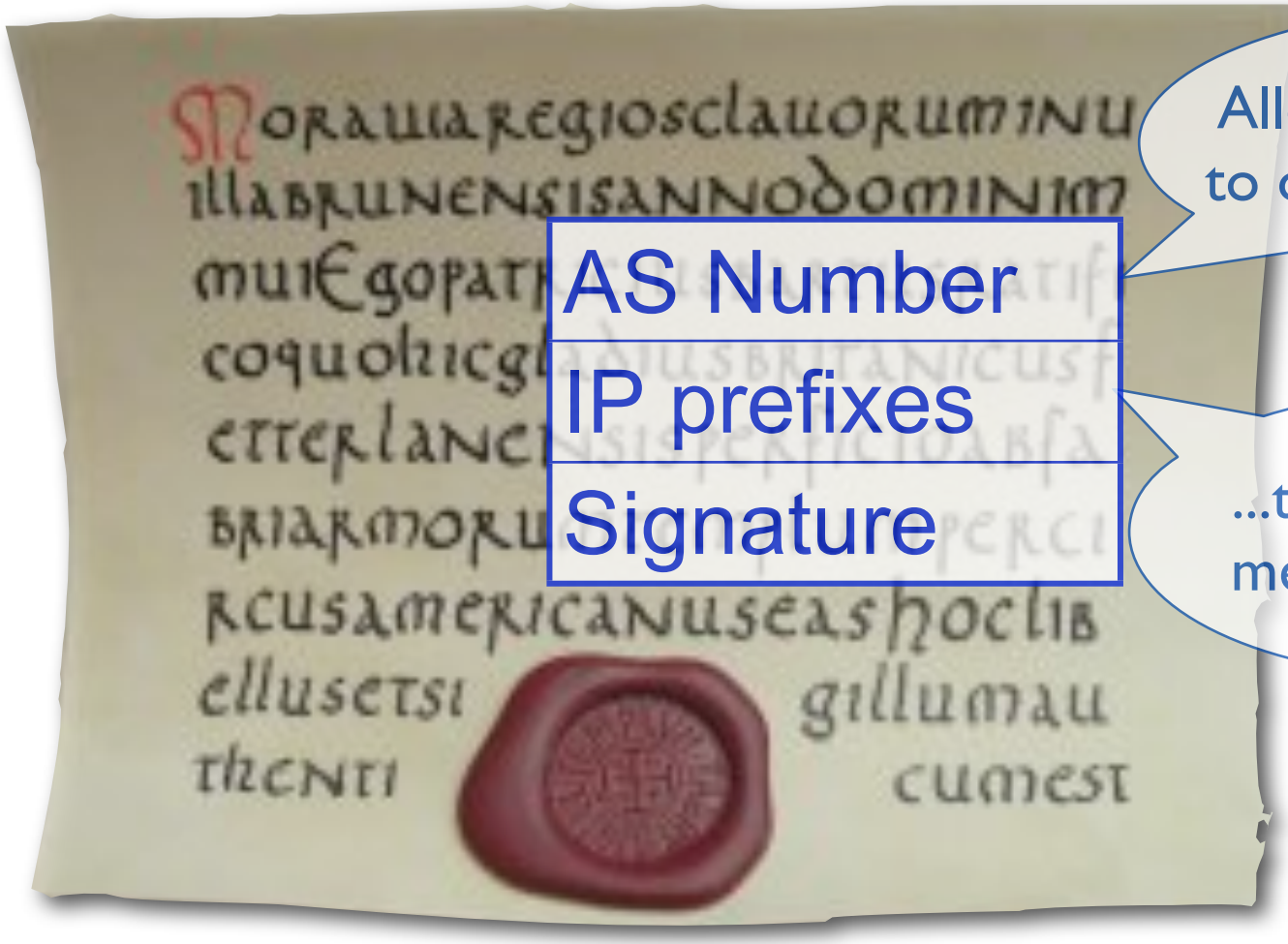
Signed object: Route Origin Authorisation (ROA)



Signed object: Route Origin Authorisation (ROA)



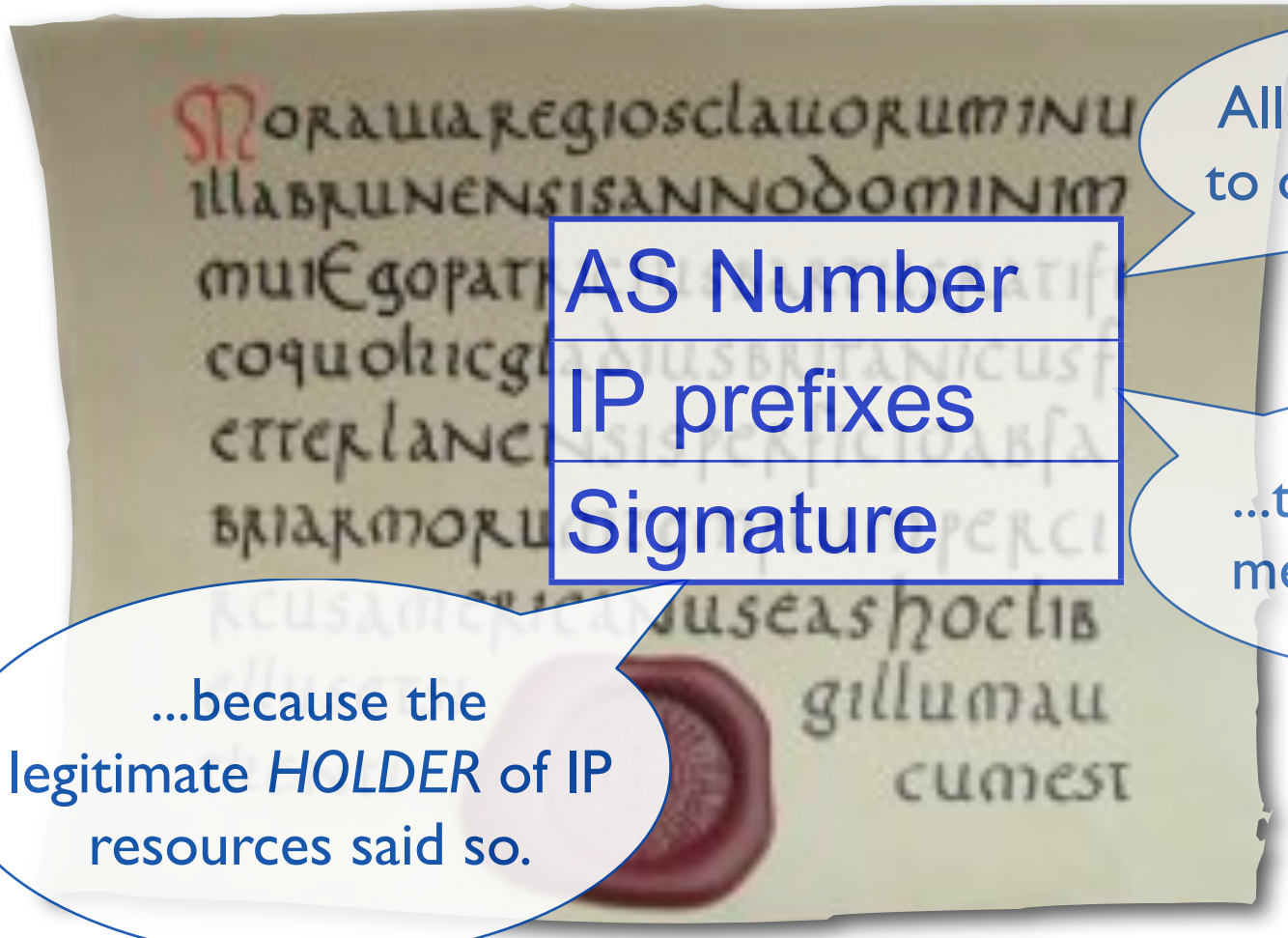
Signed object: Route Origin Authorisation (ROA)



Allow this AS Number to originate...

...the IP prefixes as mentioned here...

Signed object: Route Origin Authorisation (ROA)



AS Number

IP prefixes

Signature

Allow this AS Number to originate...

...the IP prefixes as mentioned here...

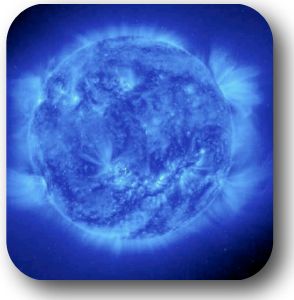
...because the legitimate *HOLDER* of IP resources said so.

What's in it for you?

- Now
  - Automated provisioning
  - Global standard
- Possible future applications
  - Resource transfers
  - Secure routing

Automated provisioning routing request

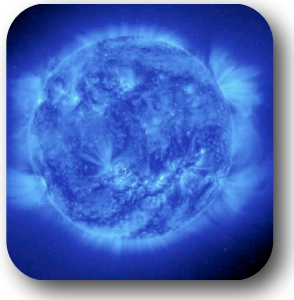
MEGACORP



BlueLight
ISP

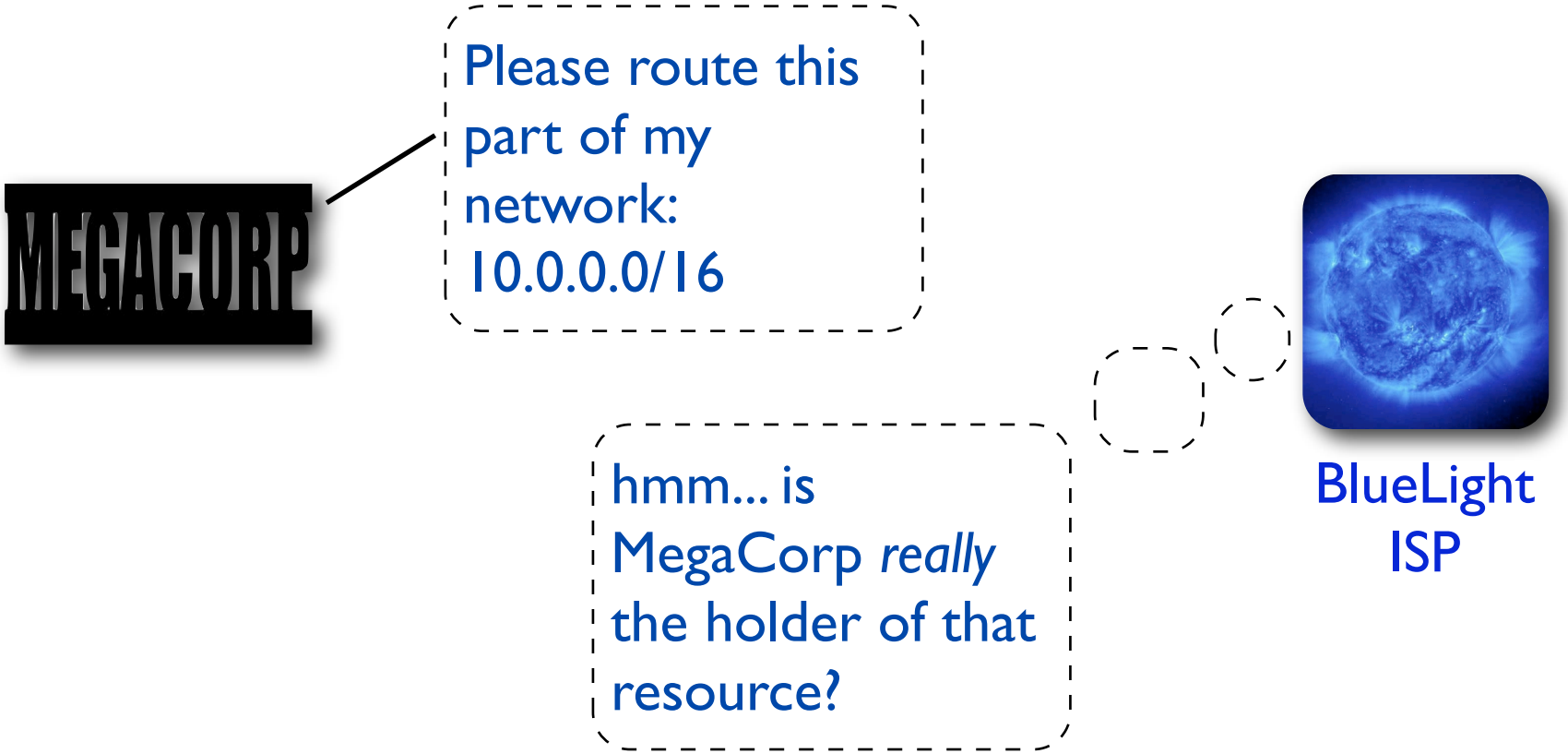
Automated provisioning routing request

Please route this part of my network: 10.0.0.0/16



BlueLight ISP

Automated provisioning routing request

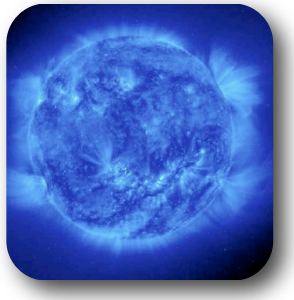


Automated provisioning

- Provisioning an IP resource
  - Does holder *really* hold the resource?
- Checking takes detective work
  - Manpower
  - Specific knowledge and skills
- Solution
  - Use ROAs

Automated provisioning routing request using ROAs

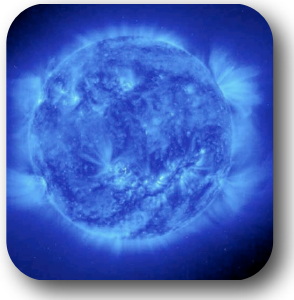
MEGACORP



BlueLight
ISP

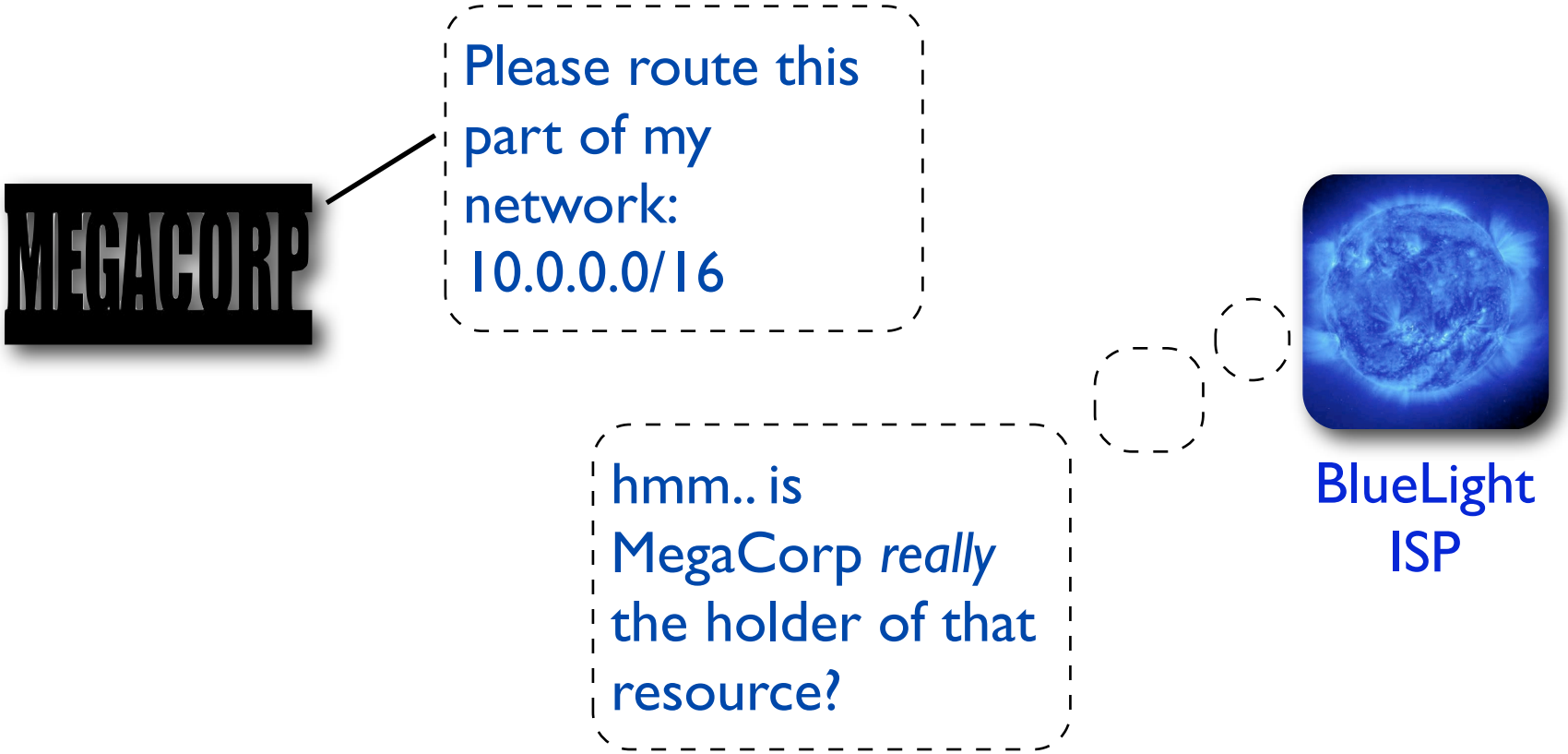
Automated provisioning routing request using ROAs

Please route this part of my network: 10.0.0.0/16



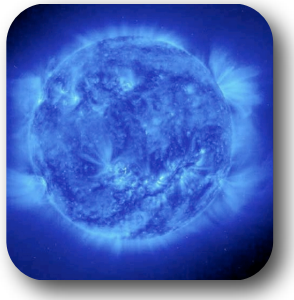
BlueLight ISP

Automated provisioning routing request using ROAs



Automated provisioning routing request using ROAs

MEGACORP

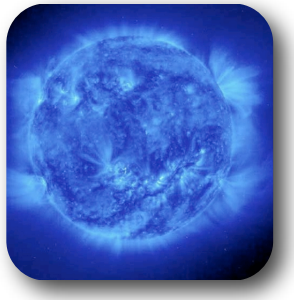


BlueLight
ISP

Automated provisioning routing request using ROAs

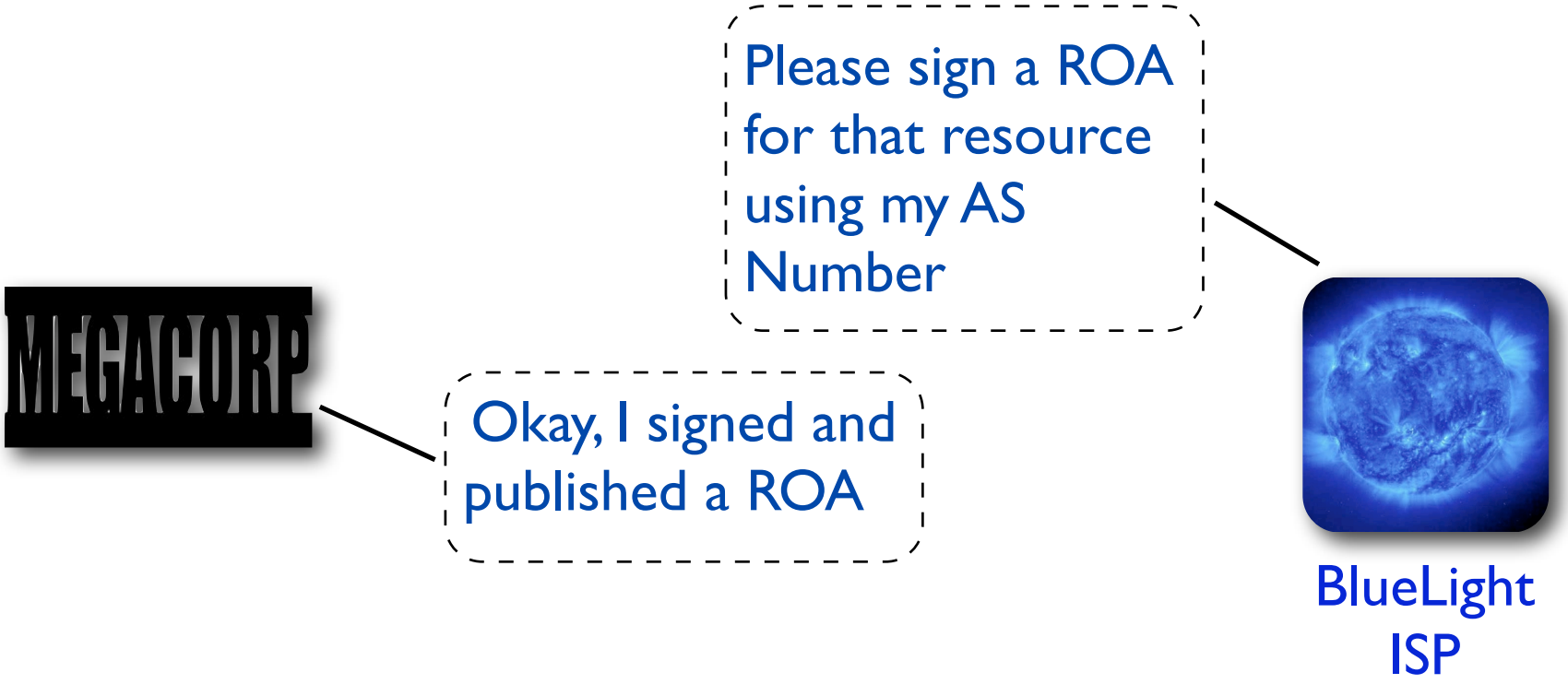
Please sign a ROA for that resource using my AS Number

MEGACORP

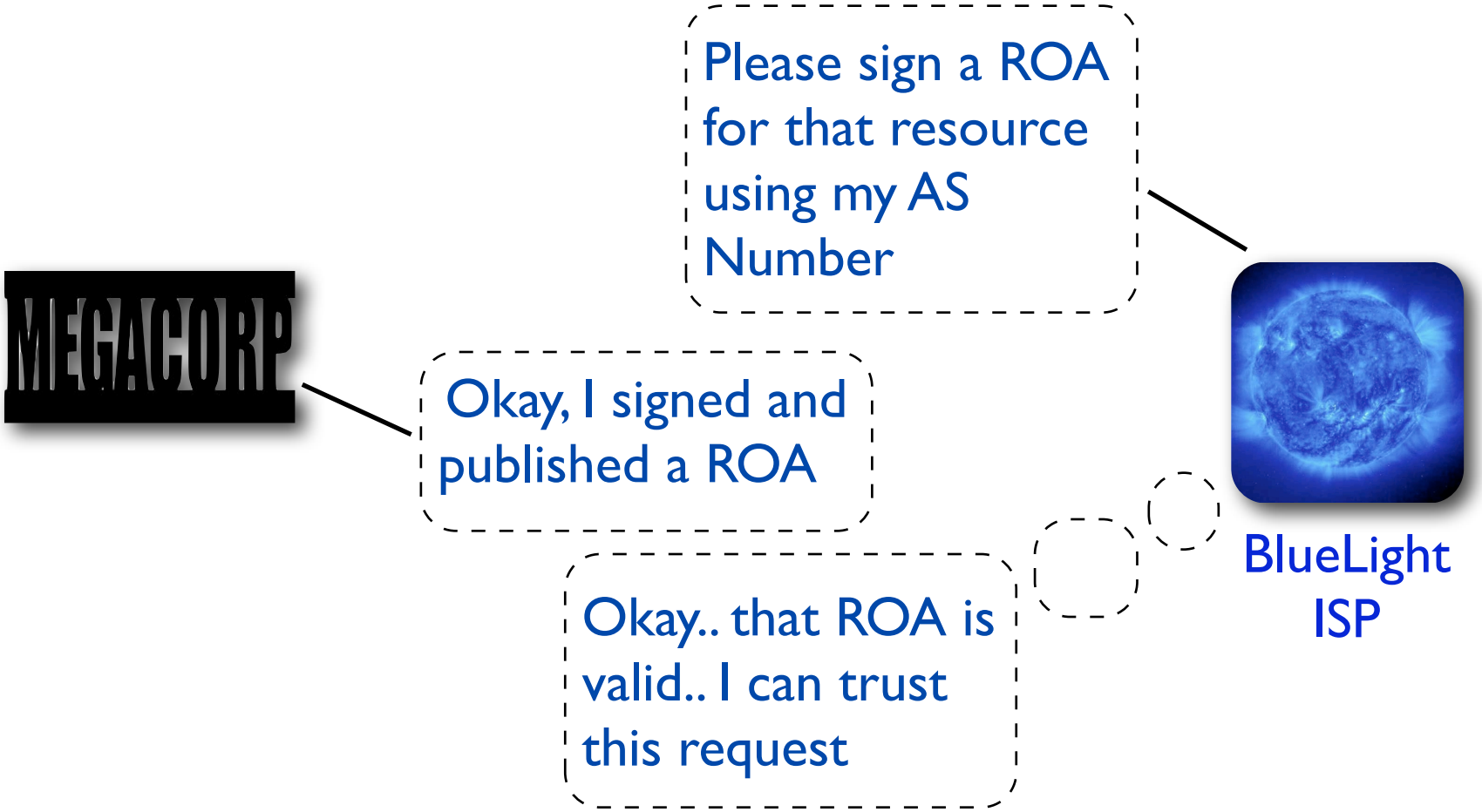


BlueLight ISP

Automated provisioning routing request using ROAs



Automated provisioning routing request using ROAs



Global standard

- Different implementations of whois like databases by different RIRs make things difficult for humans and client tools alike.
- Certification uses global standards for certificates, signed objects, publication etc.
- **NOTE:** Certification complements the current database implementations.

Demo

How we got here...

- Initial release, 30 June 2008
  - Basic key and certificate management
- Release 2, 2 September 2008
  - Manage ROAs
  - Web based ROA repository
- Release 3, 21 October 2008
  - Improved key pair life cycle management
  - Proper certificate and ROA repository (rsync)
  - Repository validated with independently developed tool

A look into the (near) future

- The road to a production system
  - Improve security (specialised crypto hardware)
  - Strong user authentication
  - Integration with LIR Portal
- Aiming for live system for all members in 2009
- Keep extending functionality incrementally
  - Web UI for validating certificates and ROA objects
  - and more...

Possible future implementations

- Further interoperability with other RIRs
- Resource transfers
- Non-hosted solutions
- Recursive model
- New types of signed objects

Finally...

- Anyone interested can join the test group
  - Talk to me
  - Go to https://certtest.ripe.net/ and sign up
  - Specify your regid to get your PA resources certified
- Advantages of testing:
  - You can help shape the application!
  - Request features, report issues

Questions?