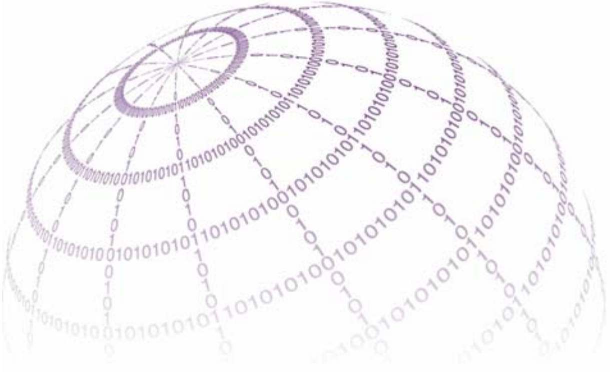


July 23, 2002

Health Care PKI Working Group:
HealthTC & M-Bridge

Center for Telecommunications and Advanced Technology

Agenda

- Overview of HealthTC Communications Model
- Discussion of M-Bridge Operations and Requirements

HealthTC (nee HealthKey)

- HealthTC (TC=Trust Communities)
  - Members of the HealthKey Collaborative
    - Foundation for Health Care Quality
    - Massachusetts Health Data Consortium (MHDC)
    - Minnesota Health Data Institute (MHDI)
    - North Carolina Health Information and Communications Alliance (NCHICA)
    - Utah Health Information Network (UHIN)
    - Community Health Information Technology Alliance of Seattle, WA (CHITA)
  - Goals:
    - “Making advances in interoperability among PKI implementations in each state”
    - “Promoting the concurrent adoption of appropriate privacy practices”

HealthTC Interoperations Concept

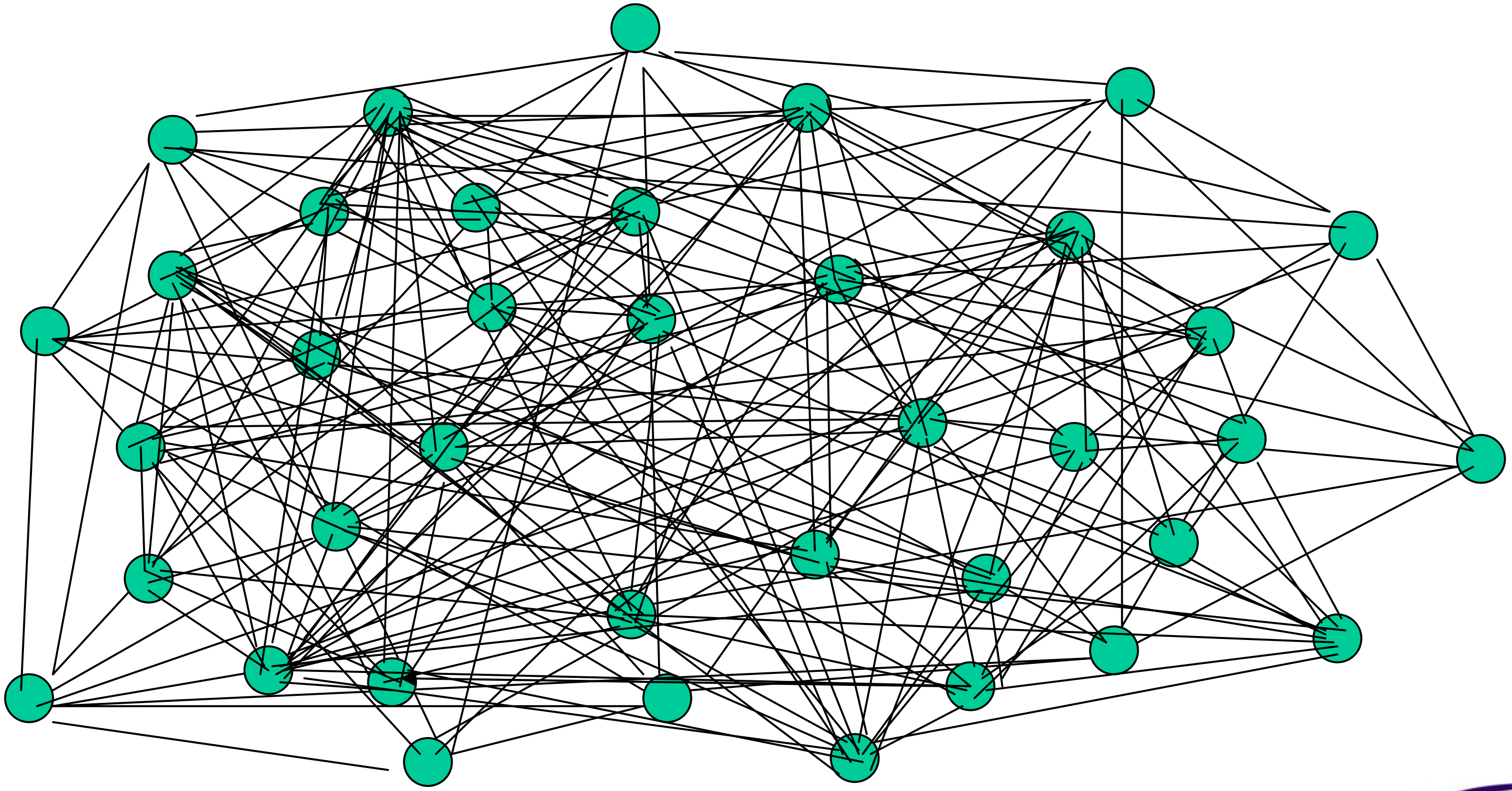
- The generic players:
  - Health care providers: local to states
  - Service providers (e.g., claims service providers, eligibility service providers): national
- Current business communications infrastructure
  - Single-provider, single-dialup solution
- Target business communications infrastructure
  - Validate certificates in digitally signed email, using enterprise-level policies
  - VPNs between participants
    - Non-IPsec; direct, as-needed, point-to-point VPNs, based on X.509v3 certificates, enabled by M-Bridge technology [OpenBridge]
- How is trust represented?
  - Brute force: via bi-lateral cross-certificates
  - More scalable: bridge membership (but is transitive trust acceptable?)

Cross-Domain Validation

3 PKI = 3 cross-certificates

10 PKI = 45 cross-certificates

100 PKI = 4950 cross-certificates

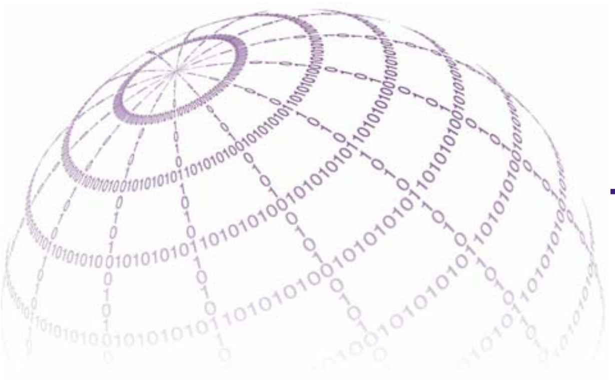


June 21, 2002

Mitretek Systems
M-Bridge

Public Key Infrastructure (PKI) Validation and Interoperability Tool and Service

Center for Telecommunications and Advanced Technology



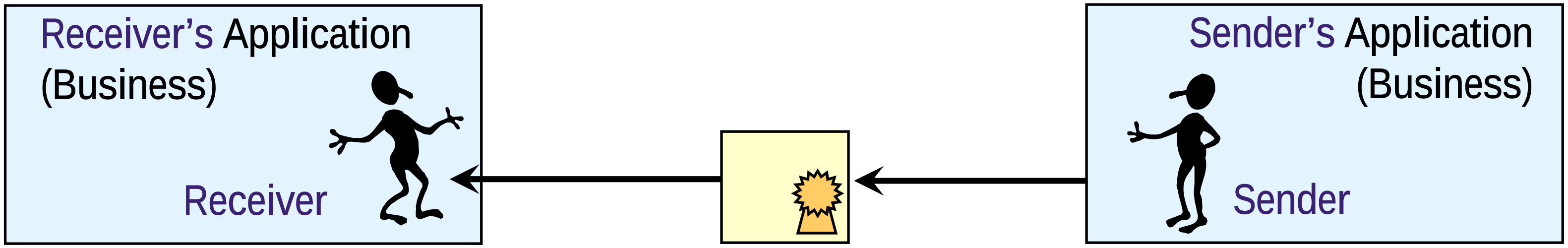
M-Bridge Overview

M-Bridge is a Certificate Validation Tool That Provides….

- Simplified PKI enabling—no end-user desktop software to maintain
- Real-time validation across disparate Certificate Authority (CA) domains, different PKI trust models, and validation protocols
- A flexible architecture of four independent components, which can be implemented individually or together to meet a variety of requirements

It's A Matter of Trust

- A digitally signed message is sent to from Sender to Receiver
- Receiver now must ask whether the digital certificate may be trusted to verify the identity of the Sender
  - Sender's certificate is not revoked
  - CA that issued Sender's certificate is trusted
    - CA signature is really from the correct CA
    - CA policies for identity proofing are acceptable
    - CA is within acceptable trust scope for Receiver

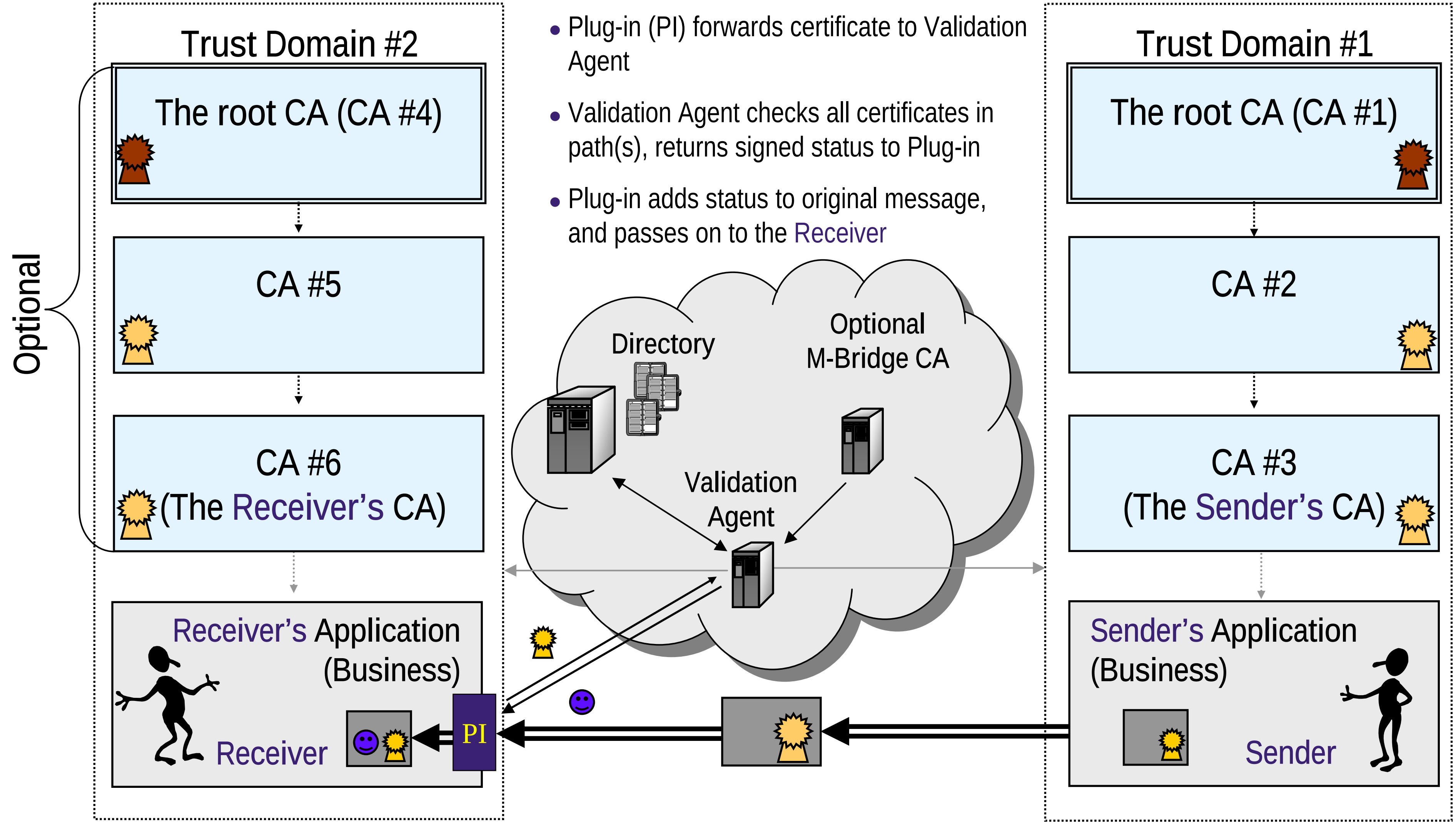

Receiver's Application (Business)
Receiver
Sender's Application (Business)
Sender

Cross-Domain Validation Via the M-Bridge

- Certificate validation
  - Status of all certificates between the Sender and Receiver is determined (valid, invalid)
  - Status is returned to Receiver
- Trust path validation
  - Receiver must trust the path of CA's established during certificate validation
  - Trust is based on determination whether the policies of Sender's domain (e.g., certificate issuance policies, security policies) meet Receiver's requirements

Certificate Validation

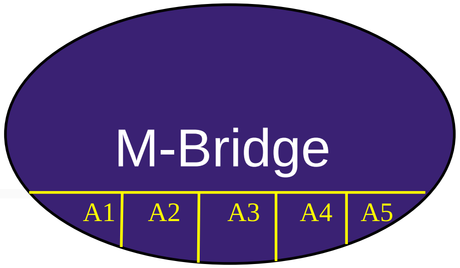
- Plug-in (PI) forwards certificate to Validation Agent
- Validation Agent checks all certificates in path(s), returns signed status to Plug-in
- Plug-in adds status to original message, and passes on to the Receiver



Trust Path Validation

Association Concept

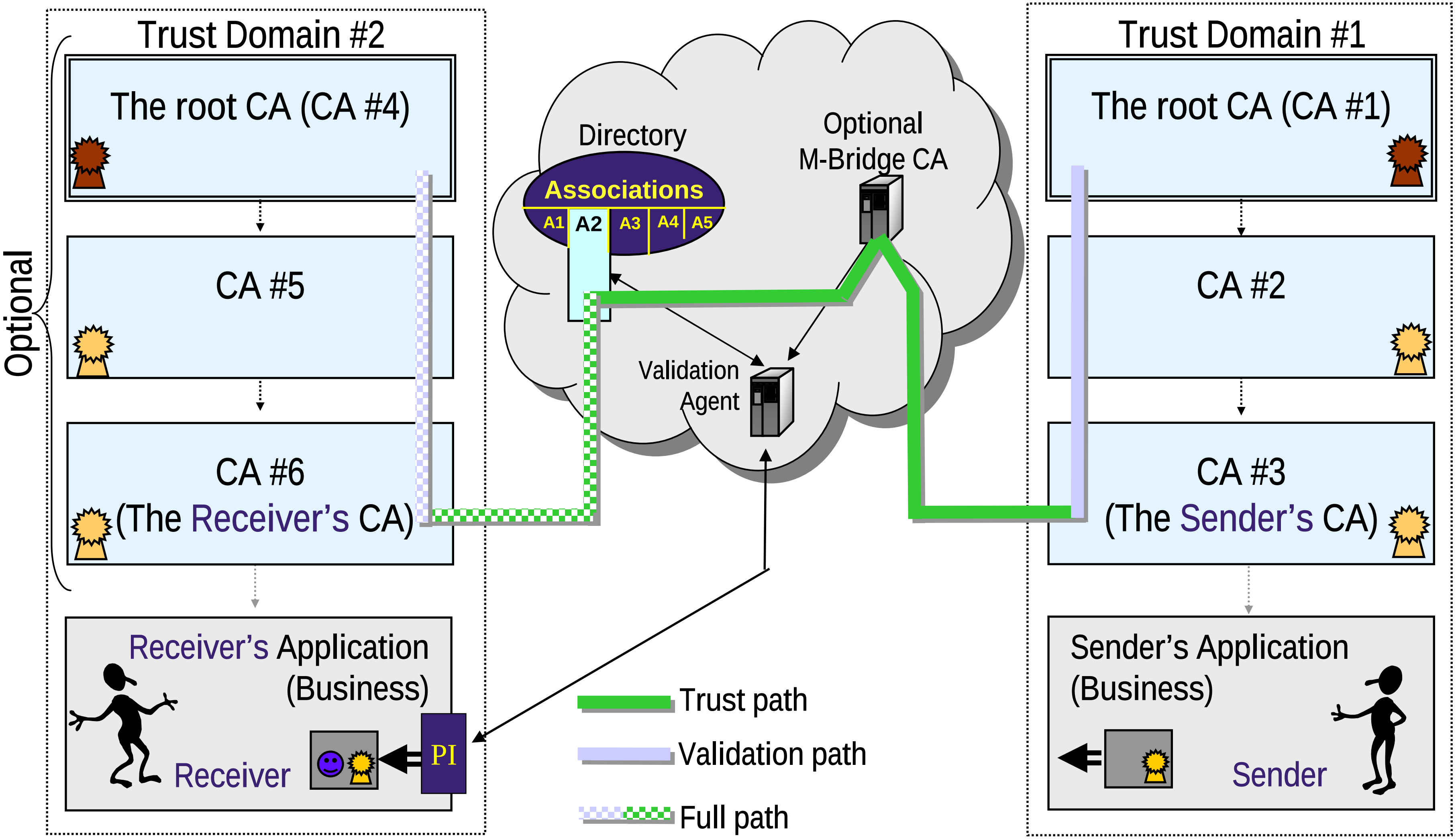
- An association is a group of CAs with similar purposes and policies
  - One association might be for law-enforcement officials only, and have strict scope rules allowing only CAs that issue to strongly authenticated law enforcement officials
  - Another association might be as generic as "the public," and have minimal requirements for CAs; existing primarily for interoperability
  - Each association has an "association policy manager" to determine which CAs to include
- Associations may support "transitive trust," but by default do not
  - Generally, CAs must directly qualify for membership
  - If an association wants to allow cross-certificate based trust transfer, this is also supported



Association Benefits

- The Receiver selects association(s) with policies suited to their trust requirements, or may create new ones
- This removes the requirement for each Receiver (or application) to maintain a trust list or individual CAs
- Provides flexibility and application control over transitive trust

M-Bridge Associations and Paths



Trust Domain #2

The root CA (CA #4)

CA #5

CA #6 (The Receiver's CA)

Optional

Receiver's Application (Business)

Receiver

PI

Directory

Associations

A1 A2 A3 A4 A5

Optional M-Bridge CA

Validation Agent

Trust Domain #1

The root CA (CA #1)

CA #2

CA #3 (The Sender's CA)

Sender's Application (Business)

Sender

Trust path

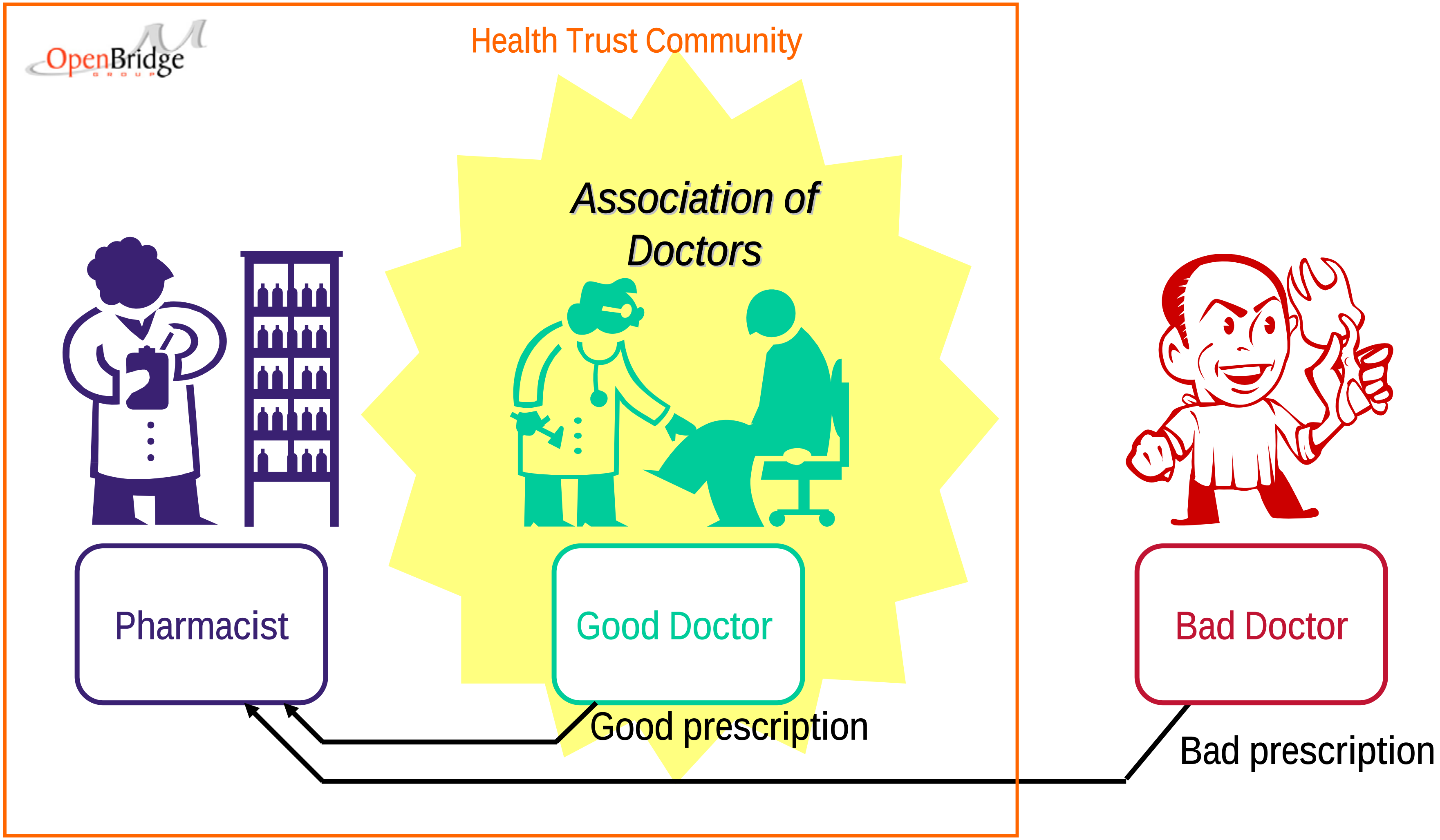
Validation path

Full path (solid => sending side only)

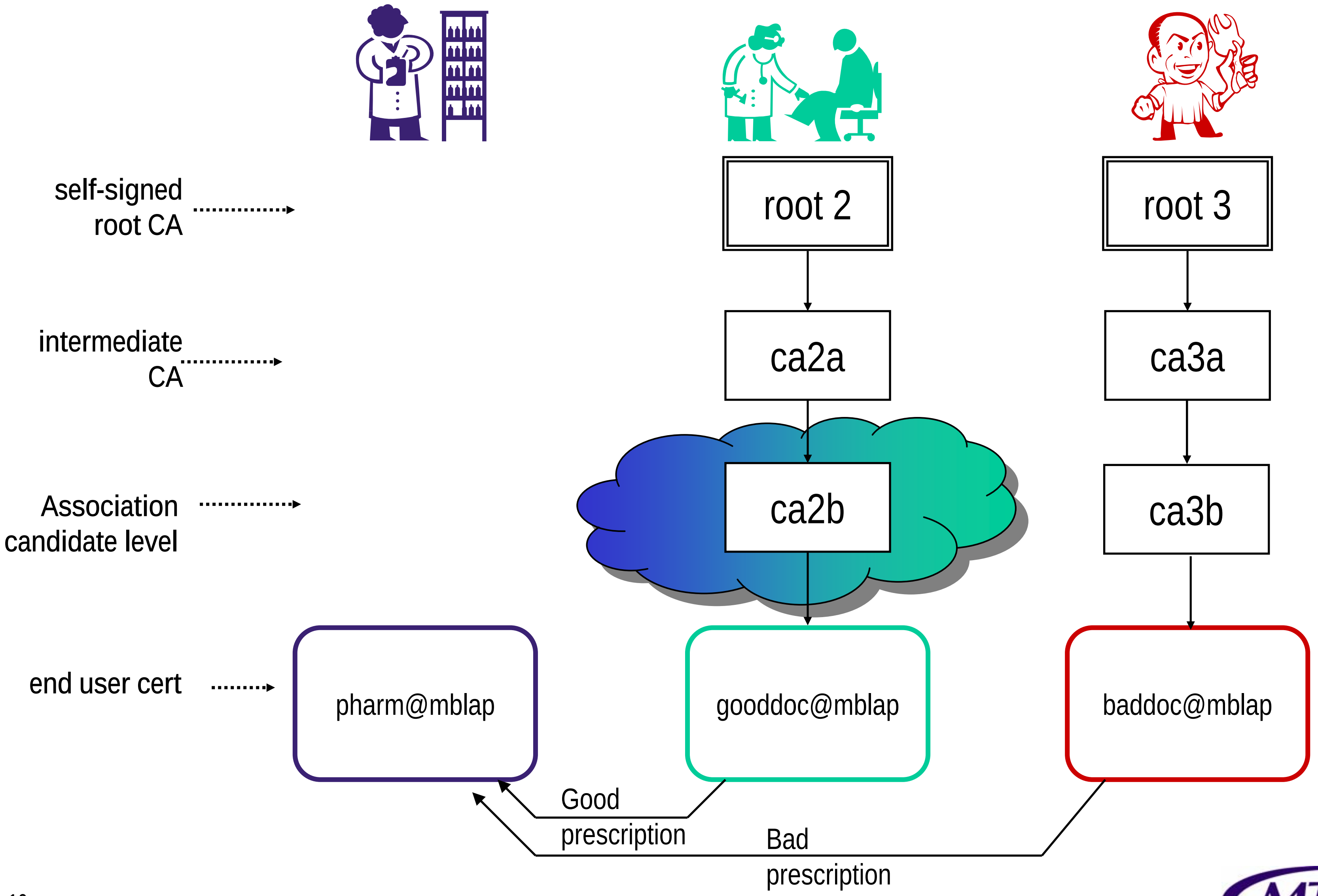
Plug-in (PI) requests assoc. “A2”

M-Bridge Demonstration Scenario

Demonstration Certificate Structure



Demonstration Certificate Structure



self-signed root CA

intermediate CA

Association candidate level

end user cert

root 2

ca2a

ca2b

root 3

ca3a

ca3b

pharm@mblap

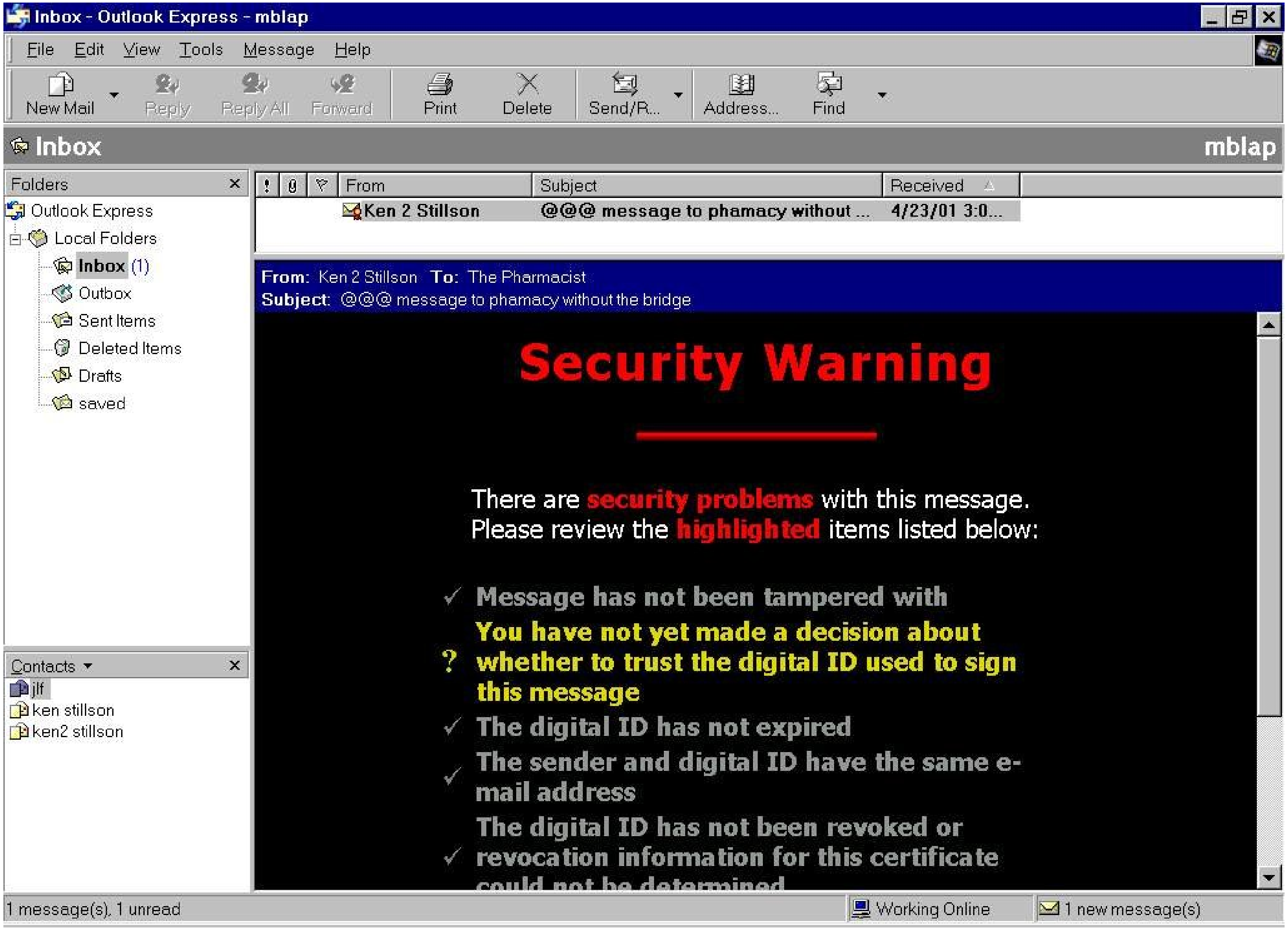
gooddoc@mblap

baddoc@mblap

Good prescription

Bad prescription

Demonstration: Without the Bridge



From	Subject	Received
Ken 2 Stillson	@@@ message to phamacy without ...	4/23/01 3:0...

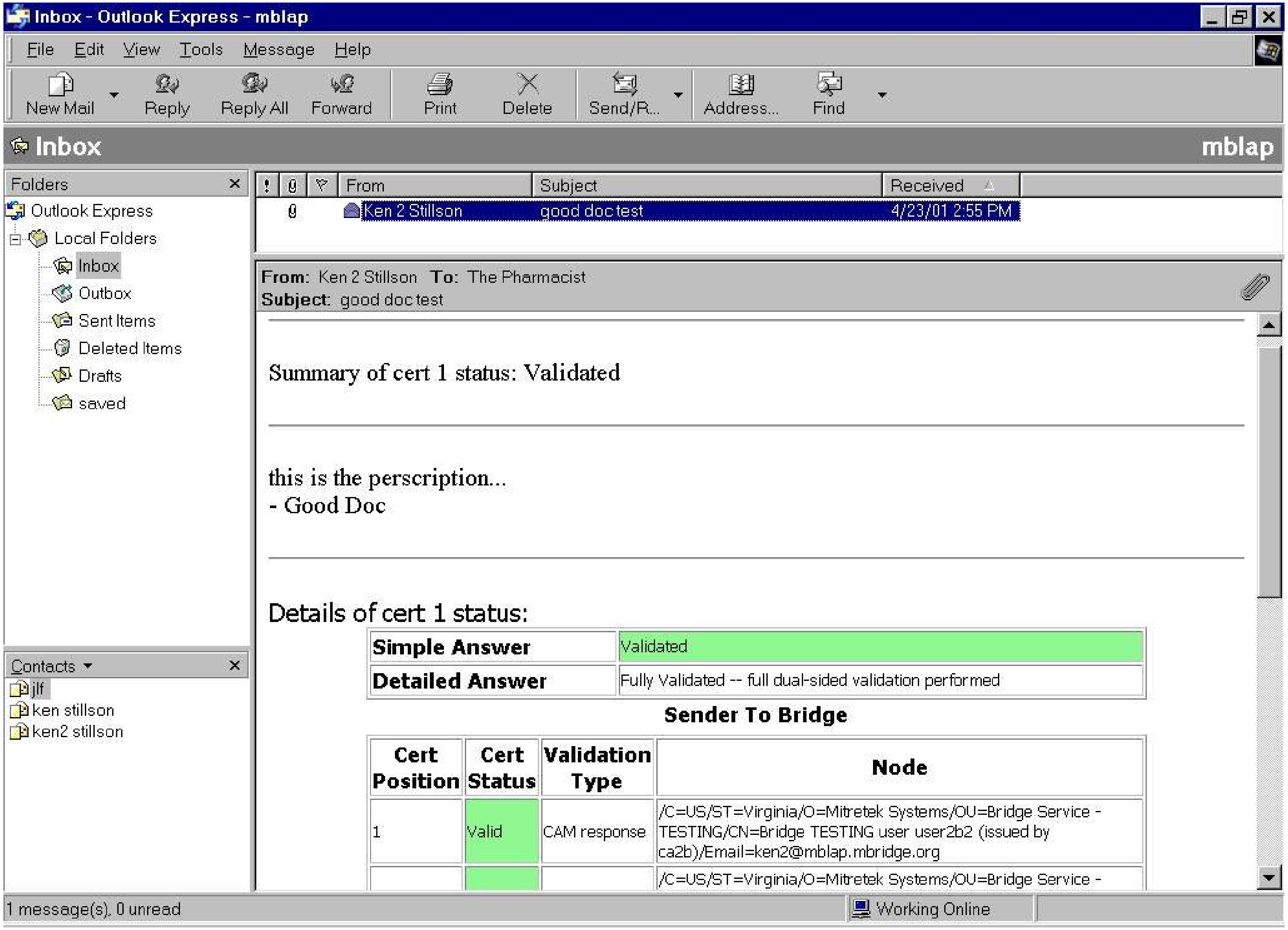
From: Ken 2 Stillson **To:** The Pharmacist
Subject: @@@ message to phamacy without the bridge

Security Warning

There are security problems with this message.
Please review the highlighted items listed below:

- ✓ Message has not been tampered with
- ? You have not yet made a decision about whether to trust the digital ID used to sign this message
- ✓ The digital ID has not expired
- ✓ The sender and digital ID have the same e-mail address
- ✓ The digital ID has not been revoked or revocation information for this certificate could not be determined

Demonstration: From the Good Doctor



!	0	▽	From	Subject	Received
	0		Ken 2 Stillson	good doc test	4/23/01 2:55 PM

From: Ken 2 Stillson **To:** The Pharmacist
Subject: good doc test

Summary of cert 1 status: Validated

this is the perscription...
- Good Doc

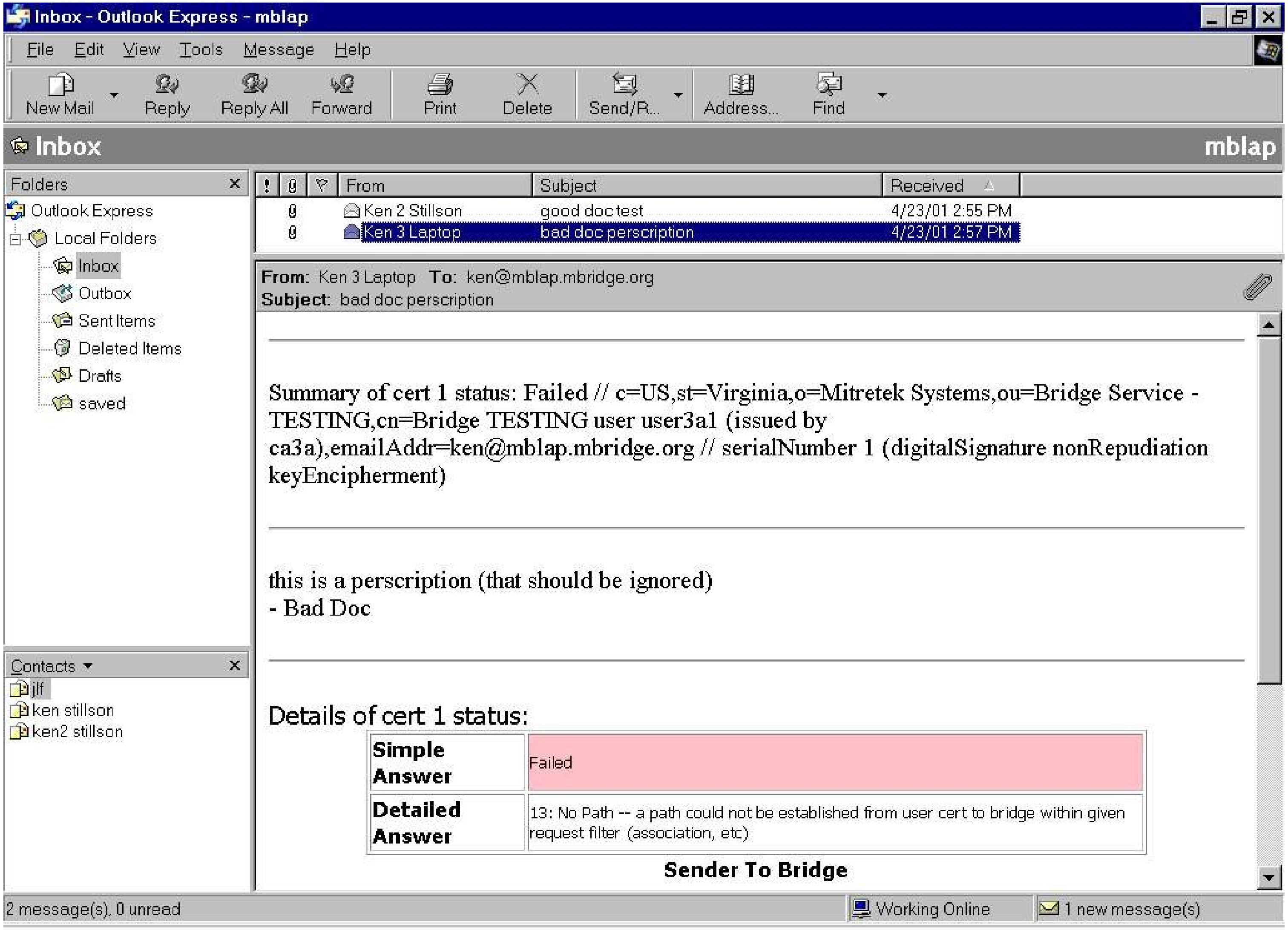
Details of cert 1 status:

Simple Answer	Validated
Detailed Answer	Fully Validated -- full dual-sided validation performed

Sender To Bridge

Cert Position	Cert Status	Validation Type	Node
1	Valid	CAM response	/C=US/ST=Virginia/O=Mitretek Systems/OU=Bridge Service - TESTING/CN=Bridge TESTING user user2b2 (issued by ca2b)/Email=ken2@mblap.mbridge.org
			/C=US/ST=Virginia/O=Mitretek Systems/OU=Bridge Service -

Demonstration: From the Bad Doctor



From	Subject	Received
Ken 2 Stillson	good doc test	4/23/01 2:55 PM
Ken 3 Laptop	bad doc perscription	4/23/01 2:57 PM

From: Ken 3 Laptop **To:** ken@mblap.mbridge.org
Subject: bad doc perscription

Summary of cert 1 status: Failed // c=US,st=Virginia,o=Mitretek Systems,ou=Bridge Service - TESTING,cn=Bridge TESTING user user3a1 (issued by ca3a),emailAddr=ken@mblap.mbridge.org // serialNumber 1 (digitalSignature nonRepudiation keyEncipherment)

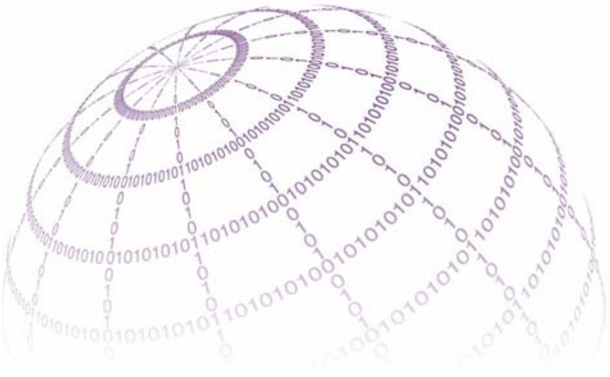
this is a perscription (that should be ignored)
- Bad Doc

Details of cert 1 status:

Simple Answer	Failed
Detailed Answer	13: No Path -- a path could not be established from user cert to bridge within given request filter (association, etc)

Sender To Bridge

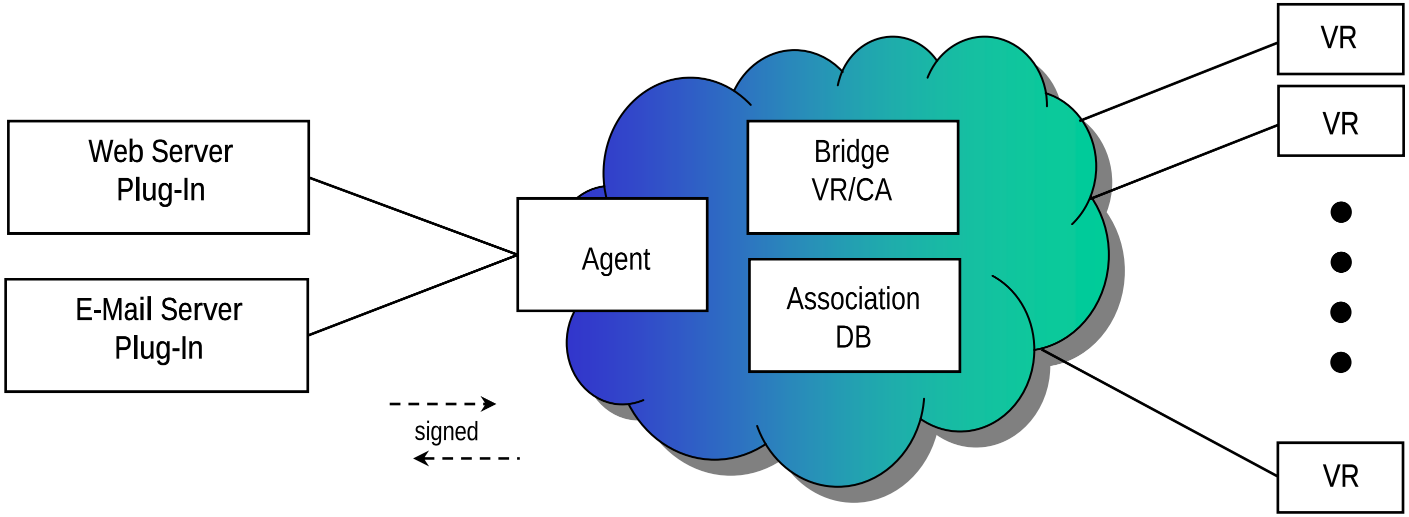
2 message(s), 0 unread   Working Online   1 new message(s)



M-Bridge System Design and Implementation

- *Plug-in Requirements*
- *Supported Validation Protocols*
- *Certificate Profiles*
- *CA Association Registration Requirements*

Overview and Requirements



M- Bridge Supplies

- Web server plug-in
- E-mail server plug-in
- Plug-in signing certificates

- ASN.1 protocol specifications for communications with Agent
- All operations inside cloud

- All communications with VR/CAs for verification services. Protocols supported:
  - CRLs
  - OCSP
  - CAM

User Supplies

- Sendmail server
- Web server

- Final determination/ approval of Association memberships

- Issuance of end-user certificates (by CA/VRs)

Plug-in System and Protocol Requirements

- E-mail server and Web server plug-ins (“thin clients”) share libraries
  - E-mail client neutral; no software changes at desktop; no policy rules management or storage at desktop
  - Small software changes at e-mail server: procmail on (or before) server redirects incoming e-mail through e-mail server plug-in (written in Perl; exportable crypto)
- Web server plug-ins
  - Apache module by VisionShare
  - Custom-VPN certificate verifier by VisionShare
  - (Could write ISAPI module)
- Edited plug-in configuration file on servers -- for: association(s) list; customer private key path; agent IP address and port (for load balancing); agent public key path

Certificate Validation Protocols

- The M-Bridge performs Internet-based real-time validation of certificate status
- CAs must provide some form of online validation service;
  standards currently supported by M-Bridge are:
  - OCSP -- with certificate AIA field containing the URL of the CA OCSP responder
  - CRL:
    - Certificate CDP (CRL Distribution Point) field containing the RFC2255 [LDAP] URI for the on-line CRL
    - Static CDP
      (CA informs bridge of this URI out-of-band; same URI for all certificates from this issuer)
  - CAM -- native
    (CA informs bridge out-of-band of CAM responder IP)
  - "Defer to DAVE"

Certificate Profile and Cryptographic Requirements

- The M-Bridge does not require a particular certificate profile (just general X509v3)
  - Individual associations within the M-Bridge may optionally require particular profile
- The M-Bridge does not require a specific X.500 directory structure or cross-chaining; any LDAP-available CRL may be accessed when CRL-based validation is in use
  - LDAP referrals: typically not needed since target directory known *a priori*
- M-Bridge may sign OCSP requests

Certificate Profile and Cryptographic Requirements (Concluded)

- For its own functions, the M-Bridge utilizes these certificate fields:
  - Issuer: to establish next link in validation path
  - AIA extension, if OCSP is to be used
  - Serial number, if CRL is to be used
  - Possibly CDP, if CRL is to be used
  - Subject, if CAM to be used
  - No other fields are processed at this time by the M-Bridge
- The M-Bridge does perform cryptographic certificate verification
  - OpenSSL is currently used; all algorithms supported by OpenSSL are understood
  - Additional algorithms may be supported as needed

CA Association Registration

- The Sender’s CA must be registered in one (or more) of the associations accepted by the Receiver
- Registration of a CA into an association is managed by the association policy manager
  - The requirements for registration with an association are set during the creation of the association
- Associations may advertise themselves via the service provider, to be available for selection by other relying parties and potential Sender’s CA’s

CA Association Registration Information Requirements

- Once admitted to an association, a CA must provide the following information to the M-Bridge:
  - Each certificate on the CA validation path, from the accepted CA up to its self-signed root CA
  - RFC2255 URI’s for on-line retrieval of those certificates
  - Instructions for on-line status checking for each of those certificates
    - No instructions needed if AIA or CDP certificate fields filled
    - Otherwise, must specify RFC2255 URI’s or CAM CA IP address(es)

CA Association Procedures

- If the association policies require full trust path validation, the CA being added to the association must also cross-certify with the M-Bridge
- M-Bridge cross-certificates (optional) are valid only within the scope of the enclosing association