GEMINI TrustEnabler

Federal PKI Technical Working Group
(FPKITWG)
25 May 2005

Peter Hesse (pmhesse@geminisecurity.com)

GEMINI TrustEnabler

Agenda

- Overview
- Problem Description
- What is TrustEnabler?
- Our target: SSL
- How TrustEnabler Works
- Today's Demo
- Conclusion

GEMINI TrustEnabler

Overview

- Public Key Infrastructure is a very useful technology for establishing trust in on-line transactions
  - SSL, VPN, Signed Forms, etc.
- "PKI-capable" implementations typically have concentrated on working well with simple PKIs
  - Single-CA environments
  - Trust lists of multiple CAs
  - Users directly issued by CAs, or through simple hierarchical relationships

GEMINI TrustEnabler

Overview (2)

- As this audience is quite aware, there are efforts to expand PKI relationships through cross-certification and Bridge certification authorities
  - Federal Bridge CA is the best-known example
  - Pharmaceutical Industry “SAFE” initiative is another
- Typical “PKI Capable” implementations are not capable of dealing with these more complicated relationships
  - Path discovery and validation implementations are incomplete

GEMINI TrustEnabler

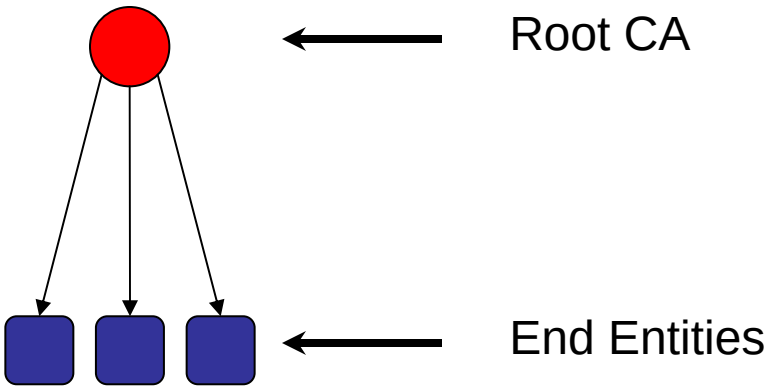
Overview (3)

- Personally, I have been working on certification path discovery and validation efforts with the U.S. Government since 1998.
  - "PKI Capable" implementations are only slightly more "Capable" now than they were in 1999!
- TrustEnabler is our first effort to reduce the delta between existing trust relationships and existing "PKI Capable" products
  - Enhance existing systems rather than replace them

GEMINI TrustEnabler

Problem Description

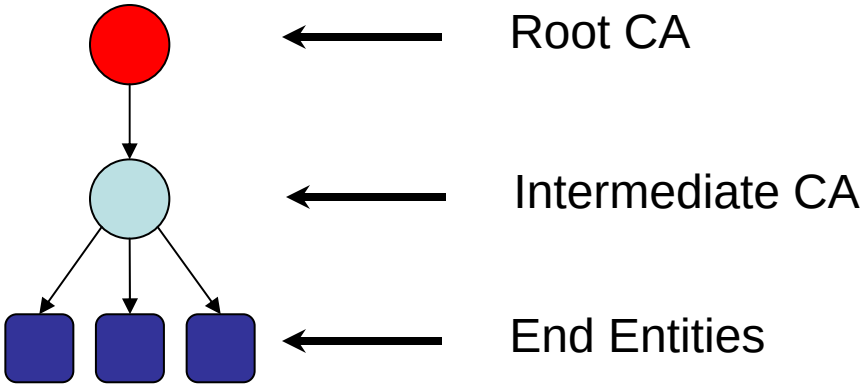
- Typical "PKI Capable" software is capable of processing simple PKIs
  - By "simple" we're talking about a flat hierarchy



GEMINI TrustEnabler

Problem Description

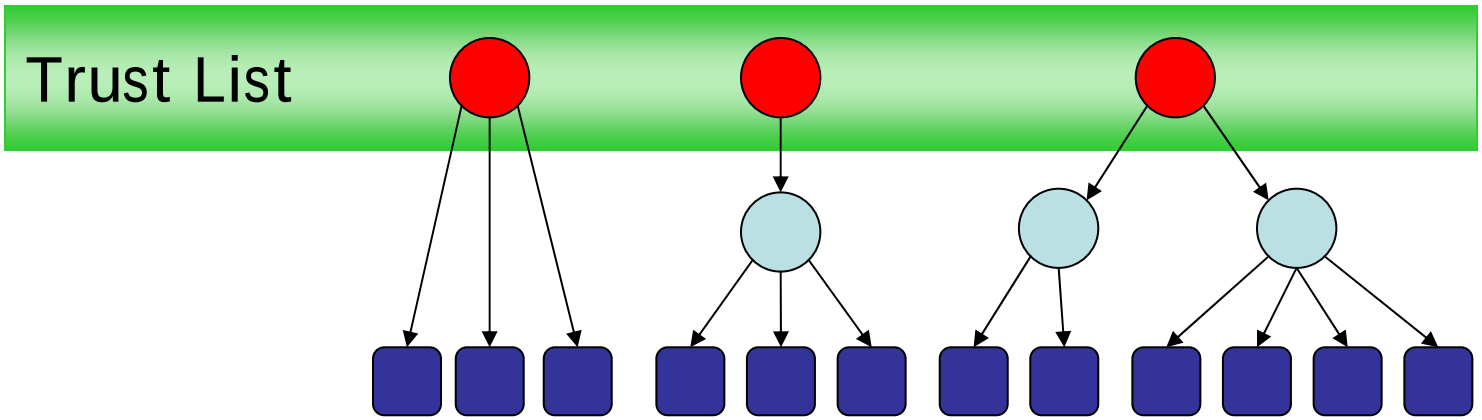
- Typical "PKI Capable" software is capable of processing simple PKIs
  - By "simple" we're talking about a flat hierarchy
  - Some support use of (known) intermediate CAs



GEMINI TrustEnabler

Problem Description

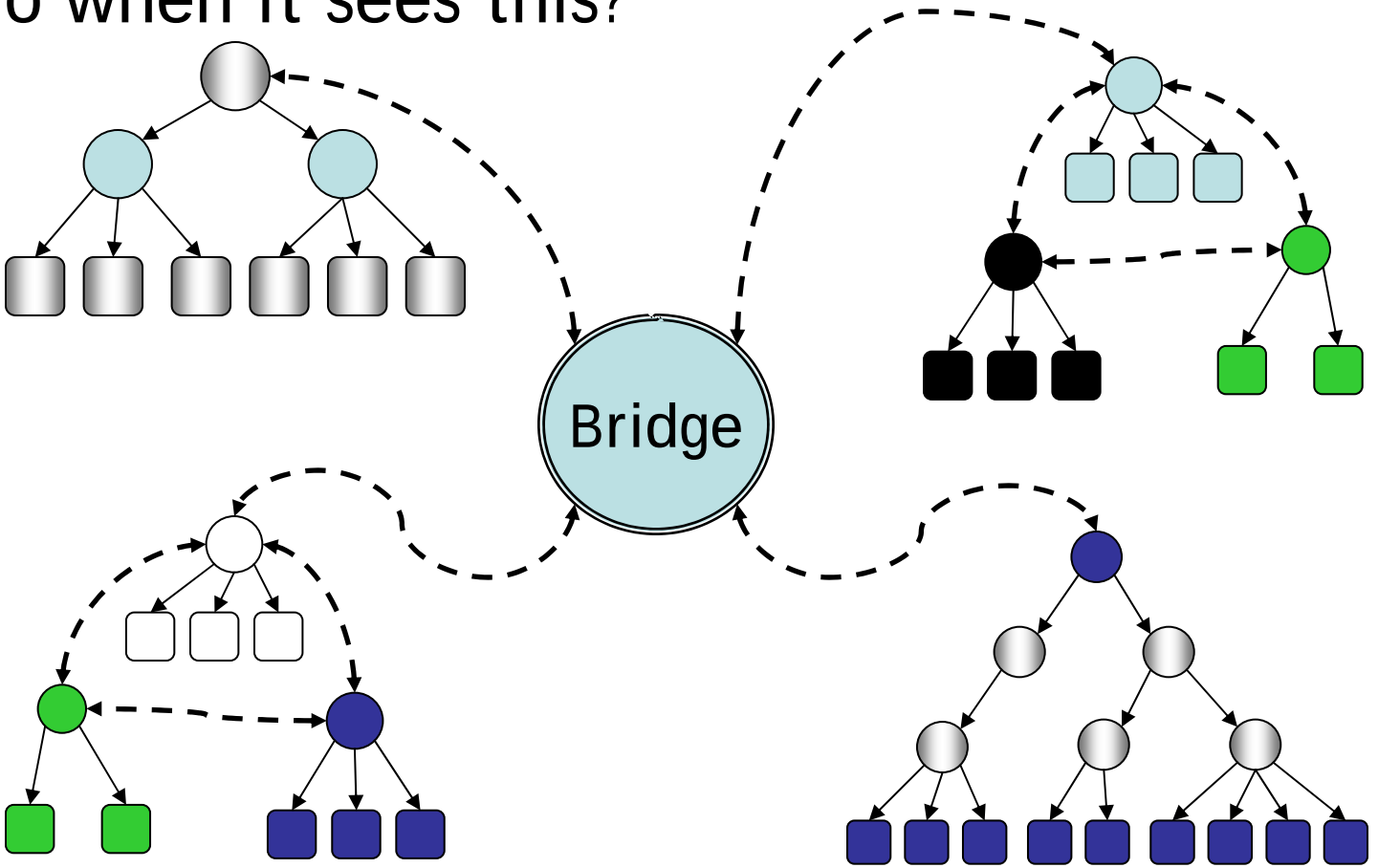
- Typical "PKI Capable" software is capable of processing simple PKIs
  - By "simple" we're talking about a flat hierarchy
  - Some support use of (known) intermediate CAs
  - Trust lists can allow multiple simple PKIs



GEMINI TrustEnabler

Problem Description (2)

- If typical software is looking for that, what will it do when it sees this?



GEMINI TrustEnabler

What is TrustEnabler?

- TrustEnabler provides services to improve the certification path discovery and validation of "PKI capable" products
- TrustEnabler is currently focused on providing a solution for applications that base their PKI capabilities around the technology of SSL with Mutual Authentication
  - Future TrustEnabler versions may expand the scope to other technologies

GEMINI TrustEnabler

What is TrustEnabler?

- TrustEnabler consists of three parts:
  - **TrustEnabler plugin**
    - Checks client's digital certificate to ensure that it is trustworthy (with full certification path validation capability)
  - **TrustEnabler Explorer**
    - Explores and stores the interconnections between PKIs (provides complex certification path discovery capability)
  - **TrustEnabler Documentation**
    - Full installation and usage documentation

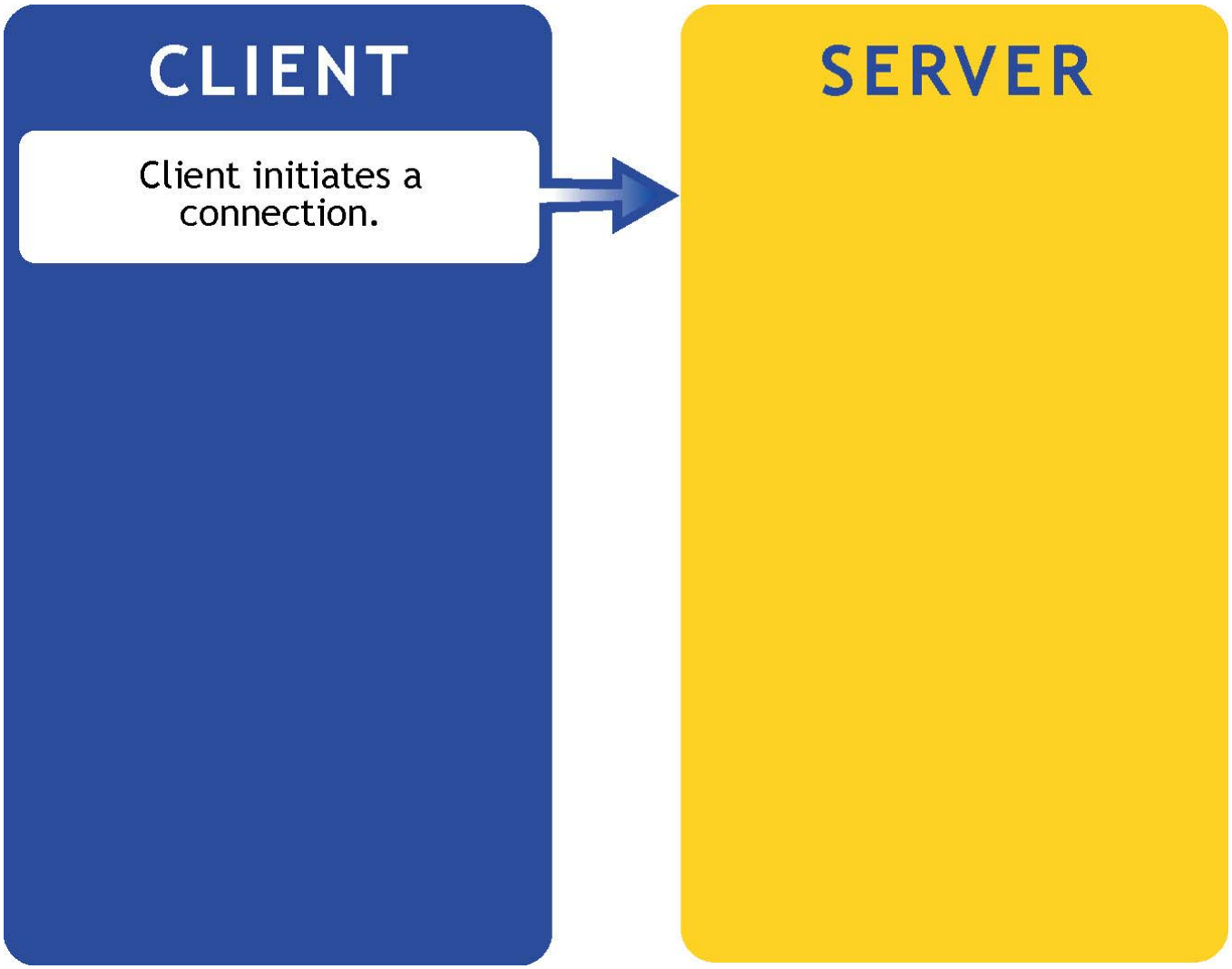
GEMINI TrustEnabler

SSL Process

- SSL with Mutual Authentication allows a user to authenticate to the server using a certificate and private key
- The following slides outline this process
  - Sometimes called Client Authenticated SSL
  - TLS also has this capability
- Also in the following slides are the impacts that the TrustEnabler software has on the process

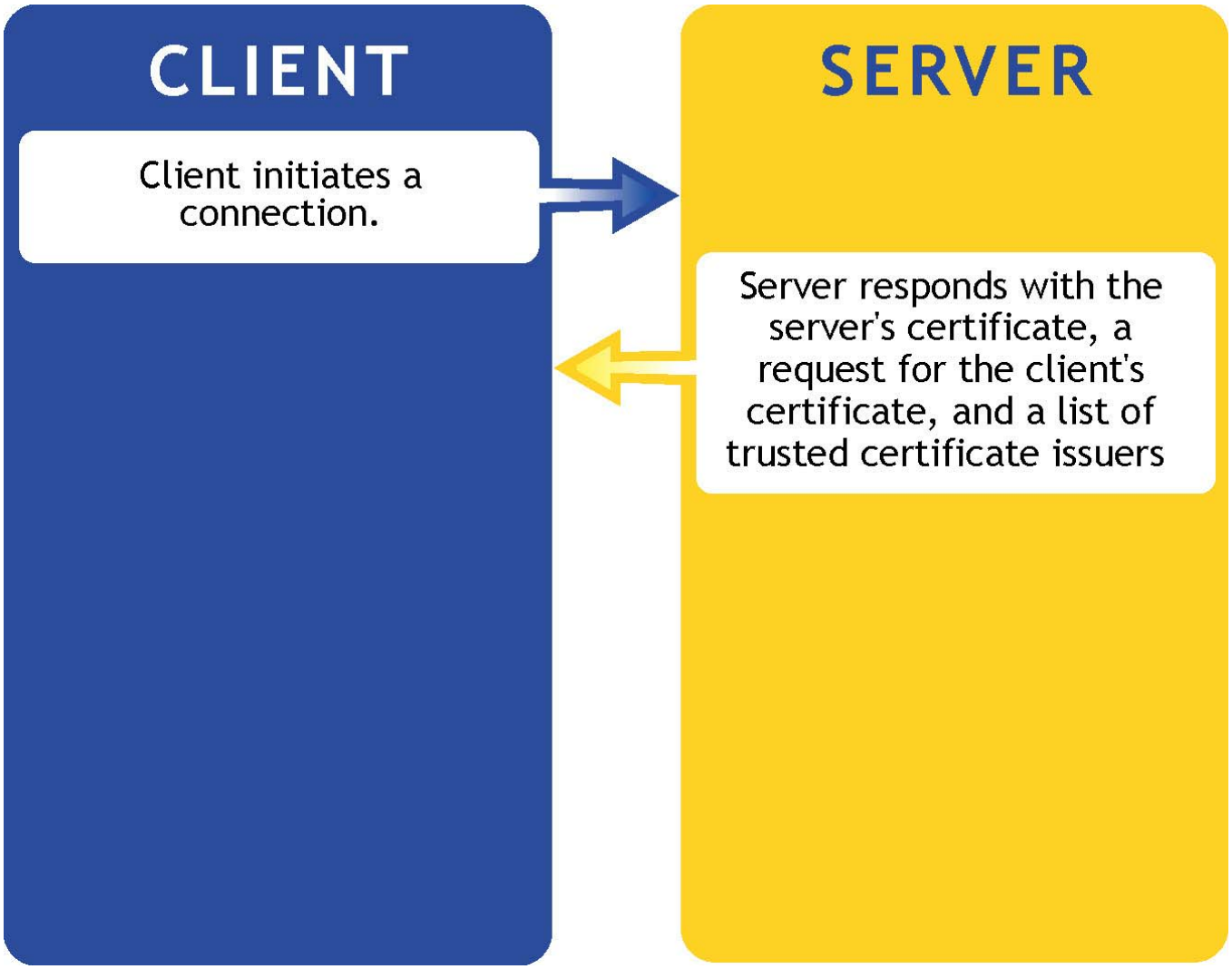
GEMINI TrustEnabler

SSL Process



GEMINI TrustEnabler

SSL Process



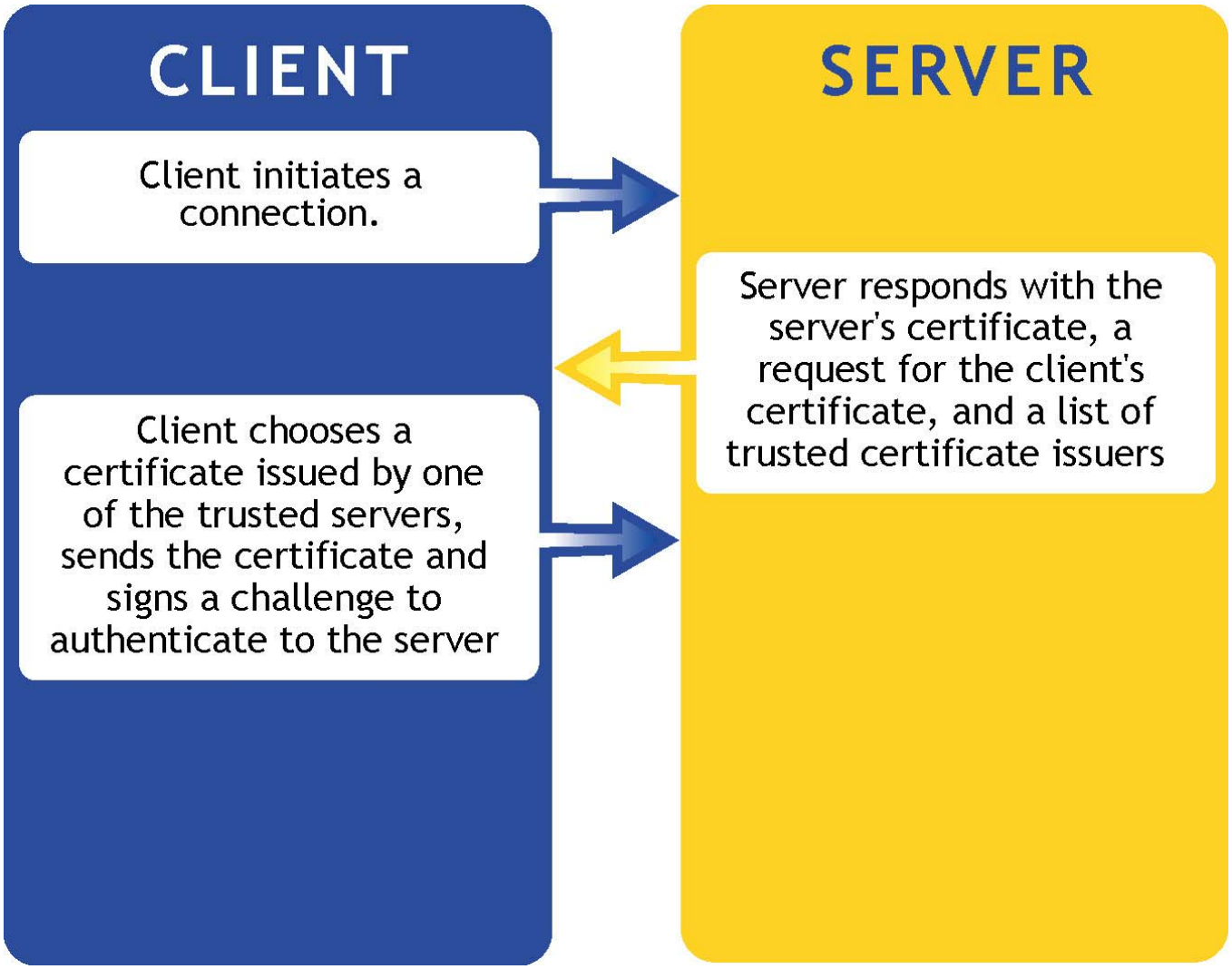
GEMINI TrustEnabler

TrustEnabler IMPACT

- Typical implementations just send the contents of the SSL server's trust list in this response
  - Trust lists typically don't know anything about complex PKIs
- **TrustEnabler Explorer** populates the SSL server's trust list with all other issuers it has found while exploring the PKI
  - This is just to enable more clients to get in the front door with their certificate
  - They won't get to the application unless the certificate can be validated back to the trust root

GEMINI TrustEnabler

SSL Process



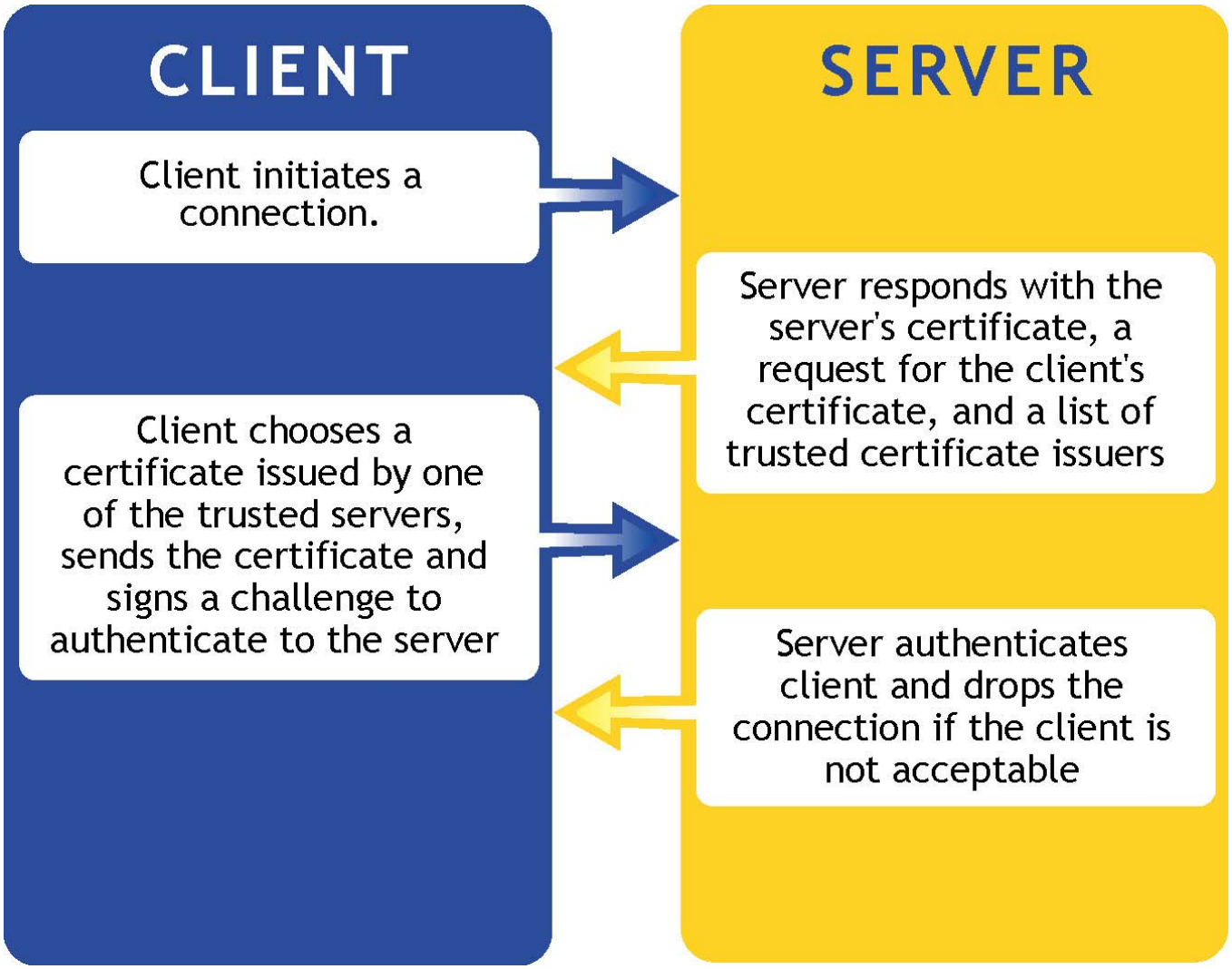
GEMINI TrustEnabler

TrustEnabler IMPACT

- In typical implementations, a user from another PKI will not be able to select their certificate
  - Unless their certificate issuer is stored in the SSL server's trust list
- Since **TrustEnabler Explorer** populated the SSL server's trust list with other issuers, the client can now select their own certificate and begin the process of authenticating to the server

GEMINI TrustEnabler

SSL Process



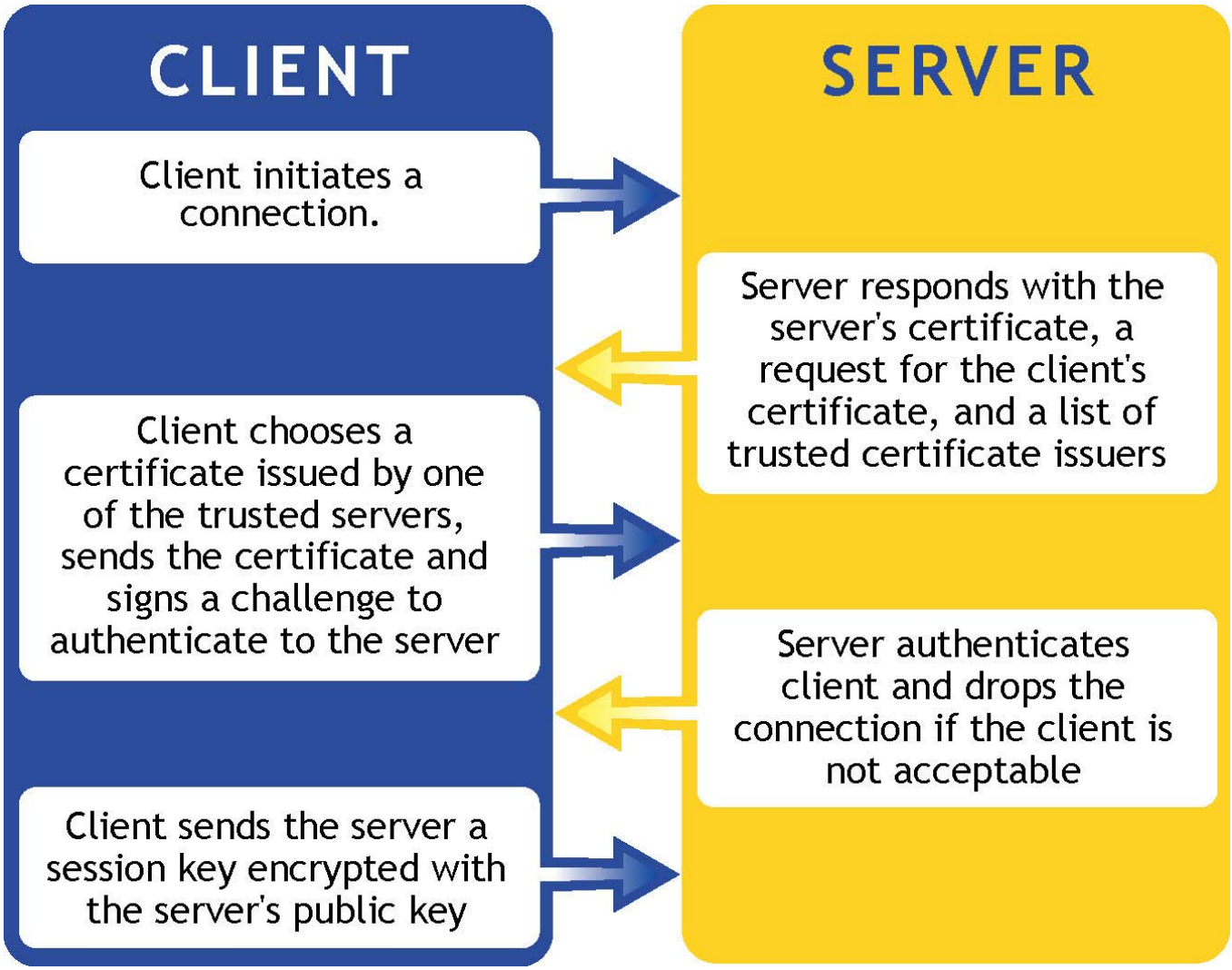
GEMINI TrustEnabler

TrustEnabler IMPACT

- Many SSL server implementations are lacking in their certification path validation capabilities
  - Some do not perform revocation checking
  - Others do not check name constraints, certificate policies, etc.
- The **TrustEnabler Plugin** provides full certification path validation capabilities to ensure that the certification path is truly valid before allowing the user to continue

GEMINI TrustEnabler

SSL Process



GEMINI TrustEnabler

How TrustEnabler Works

- The **TrustEnabler Explorer** periodically performs path development starting from one or more trusted root certificates
  - Utilizes an LDAP/X.500 directory to find relationships
  - Future versions will support SIA/AIA extensions to find additional relationships
- The discovered certificate issuers are inserted into the SSL server's trust list

GEMINI TrustEnabler

How TrustEnabler Works

- The **TrustEnabler Plugin** is an access control plugin which is invoked after the SSL negotiation process is completed, but before any pages are served to the client
  - Uses the Certificate Management Library (CML) v2.4 to perform certification path validation
- The plugin is invoked upon every request to the server
  - Validation state of client certificates is cached for a configurable amount of time to ensure responsiveness
    - Don't want to re-do validation for every request

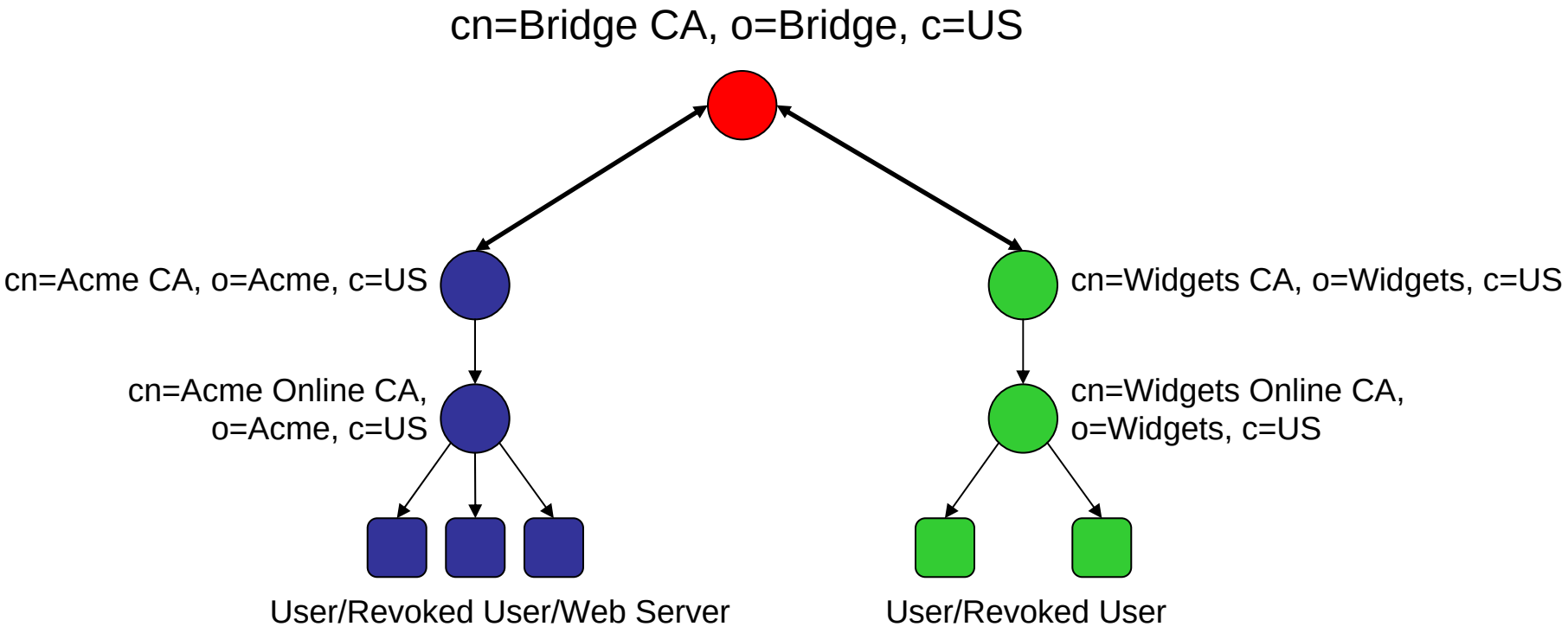
GEMINI TrustEnabler

Today's Demo

- Demonstration setup:
  - Virtual machine acting as Acme server/client
    - Windows 2000 Server SP4 / IE 6
    - OpenLDAP directory server
    - Two instances of Sun ONE Web Server 6.1 set up for SSL w/mutual authentication
      - One with TrustEnabler 1.4, one without
  - Desktop acting as Widgets server/client
    - Windows XP SP2 / IE 6

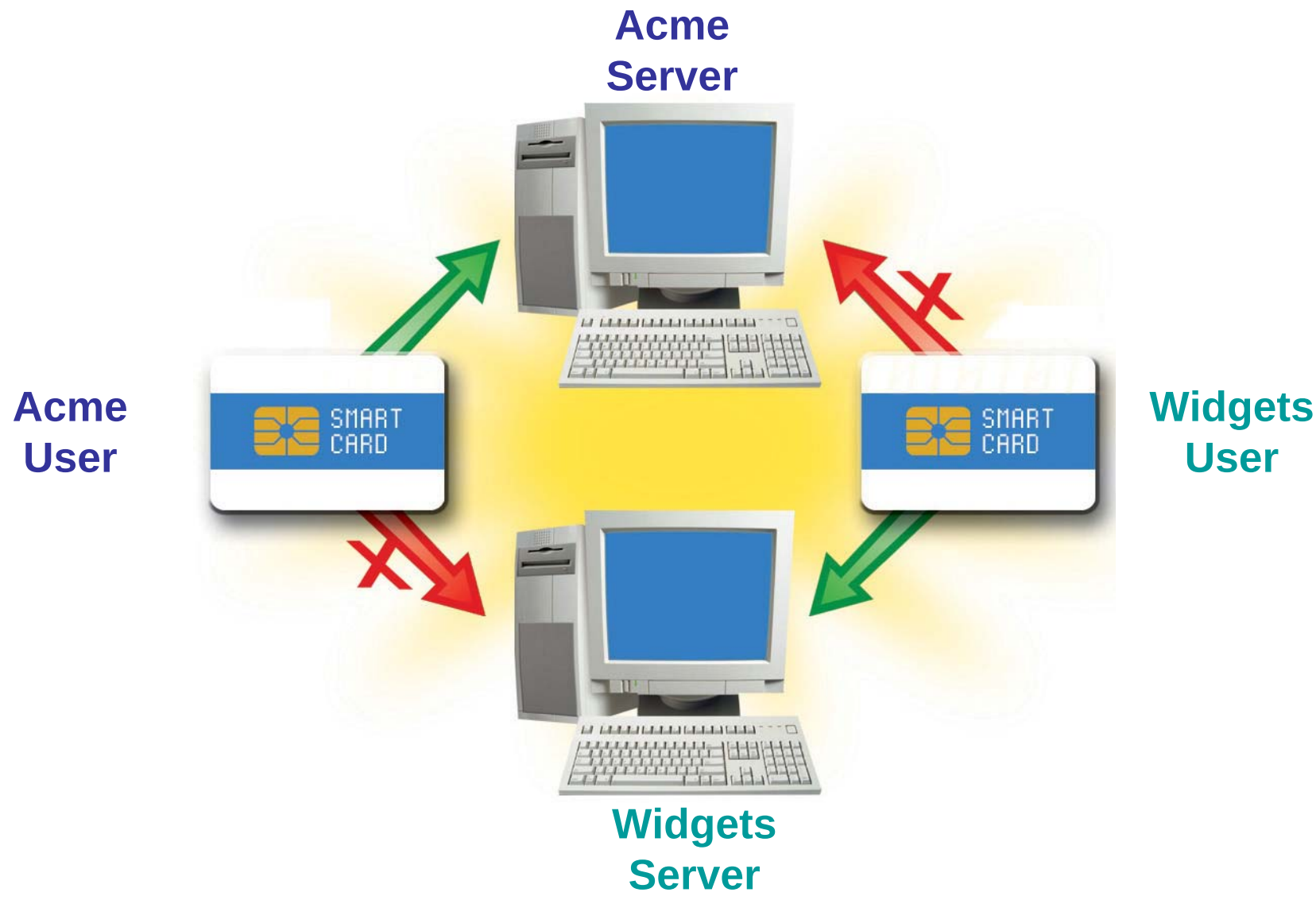
GEMINI TrustEnabler

Demonstration PKI



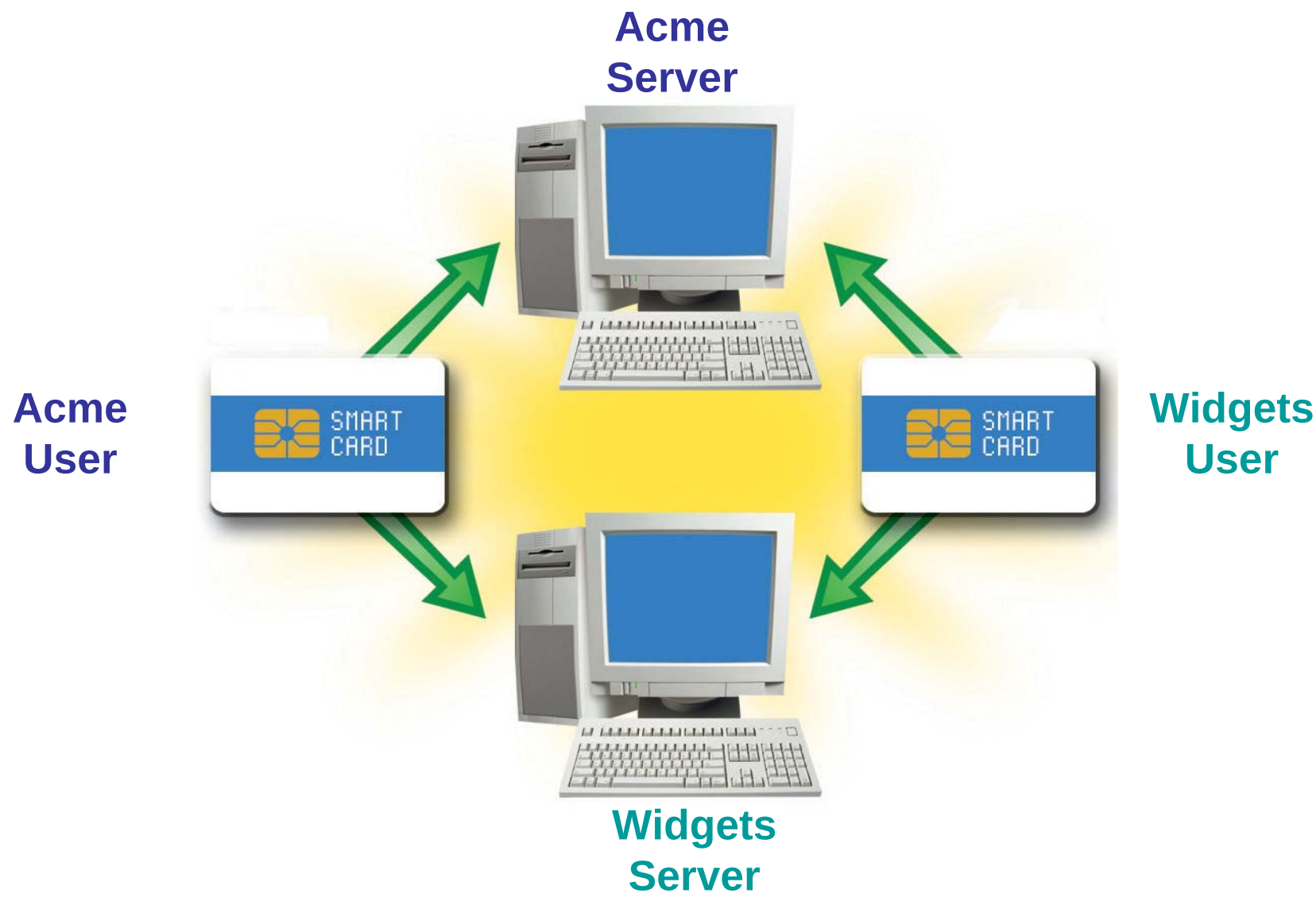
GEMINI TrustEnabler

Without TrustEnabler



GEMINI TrustEnabler

With TrustEnabler



GEMINI TrustEnabler

Today's Demo

- Demonstration points:
  - Demonstrate out-of-box behavior of Sun ONE Web Server with mutual authentication
    - Acme users (revoked or not) are permitted
    - Widgets users cannot log in
  - Demonstrate Sun ONE Web Server with TrustEnabler installed
    - Valid Acme users are permitted
    - Valid Widgets users are permitted
    - All others (revoked, other PKIs) are not permitted

DEMO

GEMINI TrustEnabler

Conclusion / Future Plans

- TrustEnabler provides a solution for enabling **today's** applications to work with the current *and growing* Federal PKI
  - Combined solution to allow a web-based application to accept and trust certificates from non-local PKIs
- TrustEnabler is currently available for the Netscape/iPlanet/SunONE series of web servers
  - Platforms include Windows, Linux, other *NIX
- Under Development:
  - SunONE on HP-UX
  - Microsoft IIS Version
  - OCSP Support

GEMINI TrustEnabler

More Information

- For more information, contact me directly, or visit our website:
  http://www.trustenabler.com

Peter Hesse, President
Gemini Security Solutions, Inc.
+1-703-378-5808
pmhesse@geminisecurity.com