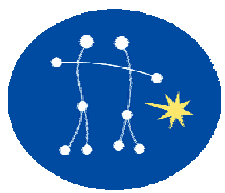
Driving Safely on Information Highway

April 2006

Orion Security Solutions



GEMINI Security Solutions

Agenda

- FIPS 201 and PK enabling
- Challenges of PK enabling
- Ways to meet the challenges
  - PKIF
  - Webcullis (demo)
  - TrustEnabler (demo)
- FIPS 201 unique PK enabling requirements
- FIPS 201 logical access solution (demo)

FIPS 201 and PK Enabling

- PKI is just one of the allowed FIPS 201 authentication mechanisms
- FIPS 201 doesn’t add many new requirements
  - Majority of the requirements persist from Federal Bridge CA enablement
    - Certificate policy processing including mappings
    - Name constraints
    - Complex path building
  - Some considerations unique to FIPS 201 are later in the presentation

Problem: Detroit Does not Build Good Automobiles

- Bad Navigation System
  - PKI toolkits do not have good certification path building capability
- Bad Steering
  - PKI toolkits perform path validation poorly, accepting bad paths causing security holes
- Bad Options
  - Applications have additional nuances hindering security and/or interoperability
    - Outlook processing S/MIME payload with foreign trust anchor
    - IE not presenting certificates that terminate to local root that does not match roots provided by SSL Server

Problem: There are Issues with the Highway As Well

- Cross-certificate formats
  - Different CA products prefer to input and output cross-certificates in different ways
    - Requires some expertise to massage the data
- Key identifiers
  - Path building software often require key identifiers to match
    - X.509/RFC 3280 don’t require it
  - CAs often generate their own key identifiers
    - Regardless of pre-existing key identifiers used in another PKI
  - RFC 4158 has guidance for CAs and path builders

Solution: GEMINI TrustEnabler

- Commercial Product
- Uses CML to augment Web Server's path building and validation features
  - PKI Enabling applications which don't know anything about PKI
- Explores trust network to provide improved hint lists to SSL clients
  - Current browsers don't build complex paths
  - Browser presented with hint list containing "Agency A Root" won't let the user choose client certificate from Agency B

TrustEnabler Features

- Certificate path discovery passes NIST PDTS
- RFC 3280-compliant client certificate path validation
- Path validation passes NIST PKITS test suite
- Product has passed PD-VAL
- Product is JITC compliant (but not certified)
- Cached validations to reduce server load for multiple requests
- Easy Configuration

Additional TrustEnabler Benefits

- Produces improved hint lists for clients
- Provides authentication information to web applications
  - Client certificate DN, issuer DN, email address parsed and provided in session variables for use by web application
  - Web application doesn’t require PKI intelligence to support PKI authentication

TrustEnabler Platforms

- Supports iPlanet / Sun ONE / Netscape web servers on Solaris, Windows, and Linux
  - HP-UX version under development
- Version with support for Apache web server on Linux is imminent

TrustEnabler Demonstration

Solution: A Few Good Men (USMC)

- PKIF – Developed by Orion for US Marine Corps
- JITC Certified
- Close to completing CC EAL 4 validation against US Government PKE PP
- Platforms
  - Windows (2000 and beyond)
  - Unix (Unix, Linux, Solaris)

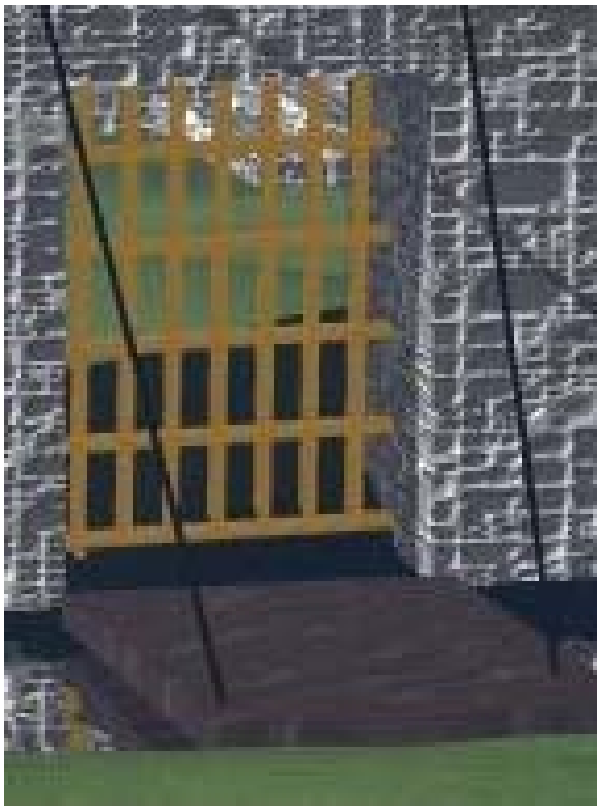
PKIF Major Features

- Cryptography
- Certificate and CRL storage and retrieval
- Certification path development in compliance with PDTS
- Certification path validation in compliance with RFC 3280 and PKITS
- Revocation status determination
- Cryptographic Message Syntax (CMS)
- RFC 3161 compliant time stamp
- RFC 2560 compliant OCSP client
- Sample GUI elements

Solution: Webcullis

- Funded by DoD
- Use PKIF to augment Web Server's path building and validation features
- Give server administrators control over which CAs should be trusted to identify users for their applications
  - Trust only Enterprise Root for path development and validation
  - Environment trust store can be used for other purposes such as providing them to IE

Why the name?



- When a bridge is in place, a portcullis is used to restrict entry to fortified structures.
- TLS-protected web sites have the same problem, especially in Bridge environment

Webcullis Features

- Certificate path discovery passes NIST PDTS
- RFC 3280-compliant client certificate path validation
- Path validation passes NIST PKITS test suite
- Product has passed PD-VAL
- Product is JITC compliant
- Underlying toolkit close to obtaining CC EAL 4 validation against the US Government PKE PP
- Cached validations to reduce server load for multiple requests
- Easy Configuration

Granular Control

- Access may be restricted based on
  - Distinguished Name
    - Name spaces at the agency level may be explicitly permitted or excluded
    - Even down to specific users
  - Certificate Policies
  - Client Key Size
  - Extended Key Usage
  - Other fields in the certificate (e.g., nationality)
- Different server resources can be configured with different restrictions

Additional Benefits

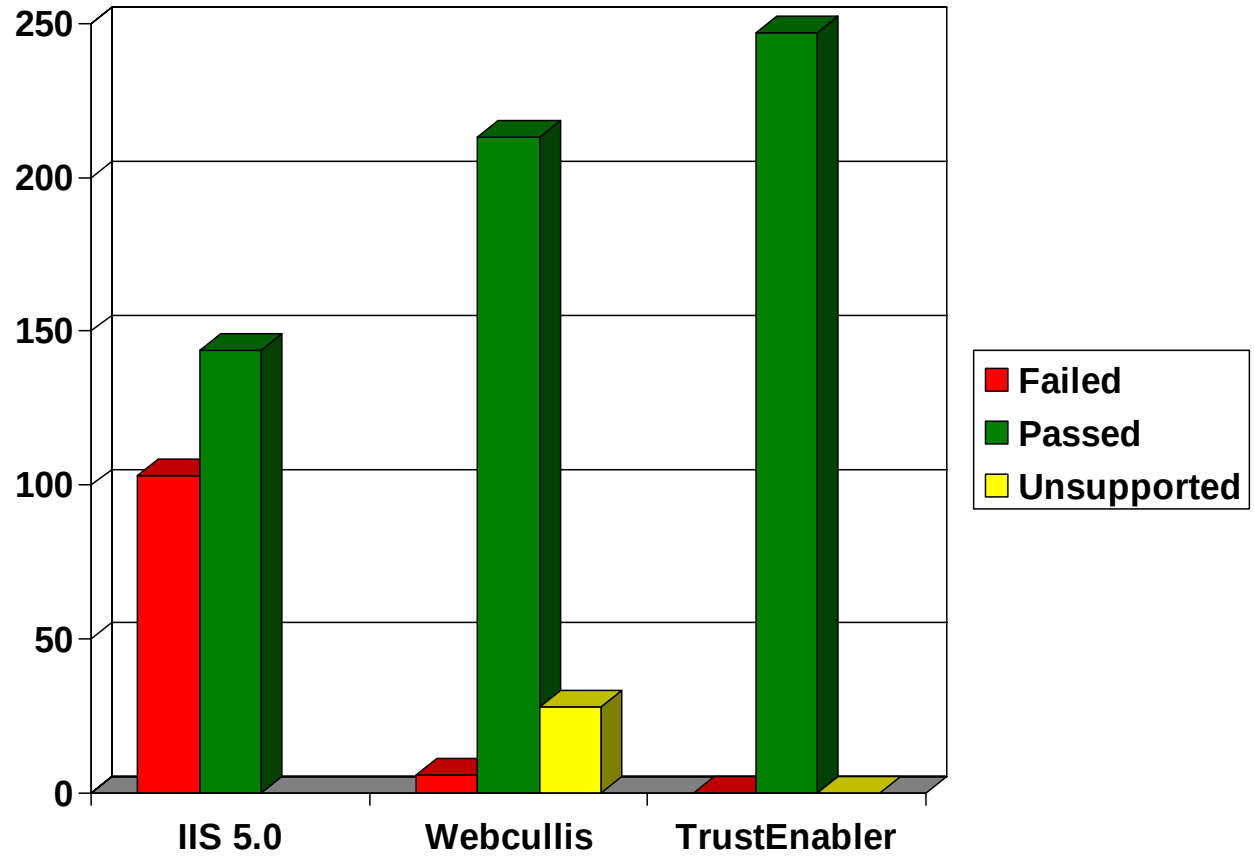
- Reliable source of authentication information
  - Facilitates integration of PKI and web applications (Portals, CMS, etc.)
  - This integration simplifies deployment of new web applications

Development Notes

- Can work around OS bugs
- Vast improvements in PKITS compliance for nearly free
- Vastly simplified validation logic
  - Core validation routine <150 physical LOC!

Webcullis Demonstration

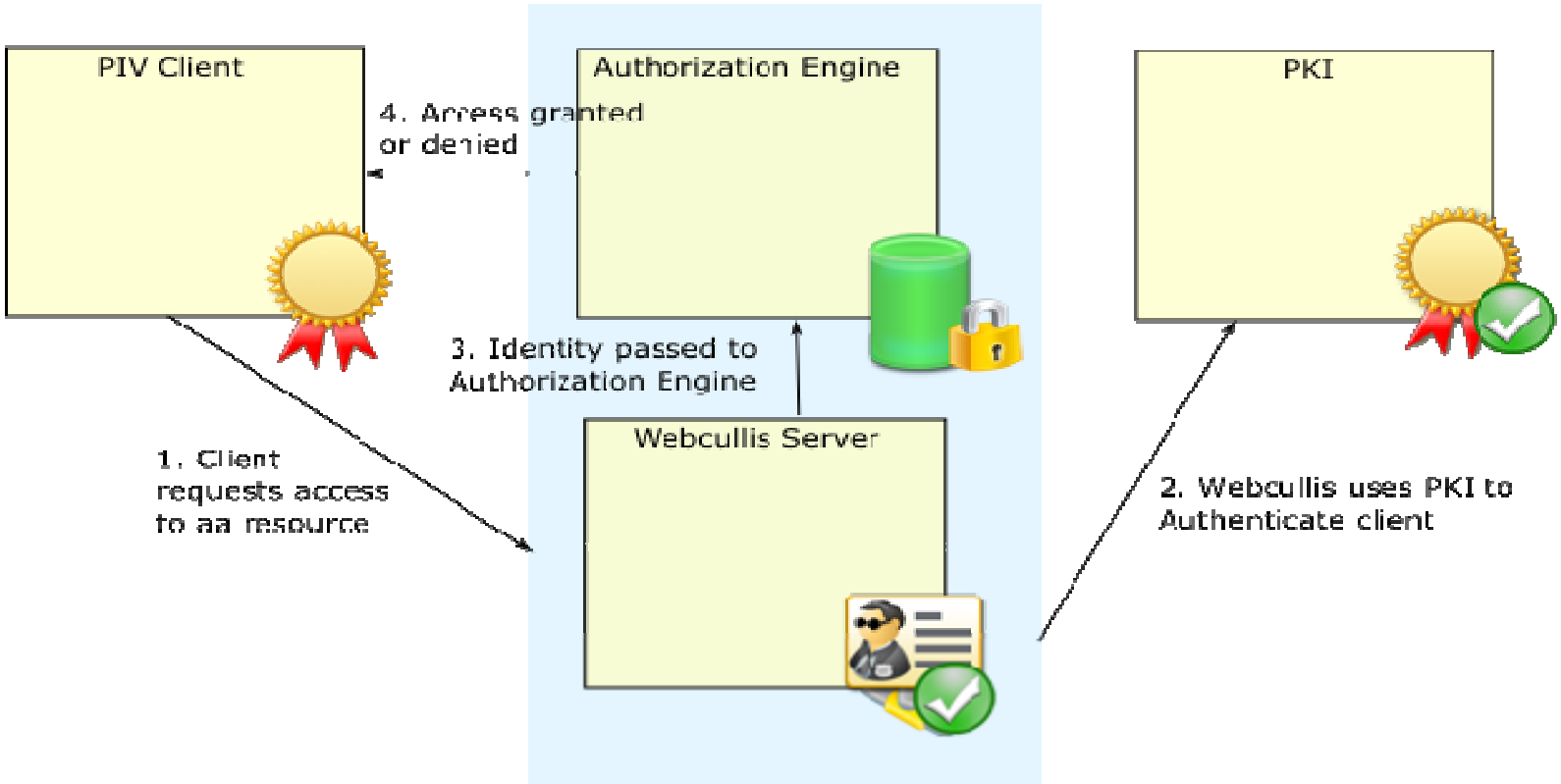
PKITS Test Results



HSPD-12 Unique PK Enabling Requirements

- SHA 256 Support ASAP (NLT 12/31/2010)
- CHUID Processing
  - Signature verification not required but desired. Also verify the signer has the appropriate EKU, i.e., PIV content signing.
- PIV Authentication Key Certificate
  - Verify FASC-N in Subject Alternative Name field
  - Verify common authentication policy OID, if PIN is not required to use the private key
- Biometric Processing
  - Verify Signature
  - Also verify the signer has the appropriate EKU, i.e., PIV content signing.
- CA use specific policy (common hardware) and under Common Root. Legacy

FIPS 201 Logical Authentication Demonstration



Summary

- PK enabling is possible and is made easier with available products and toolkits
- PK enabling does not have to cost an arm and a leg
- PK enabling does not require multi-billion dollar software company or government contractor
- PK enabling effectively and with reasonable cost requires hiring knowledgeable people
- PK enabling for FIPS 201 can be easy and inexpensive
  - Took 10 staff hours to develop the logical authentication demo