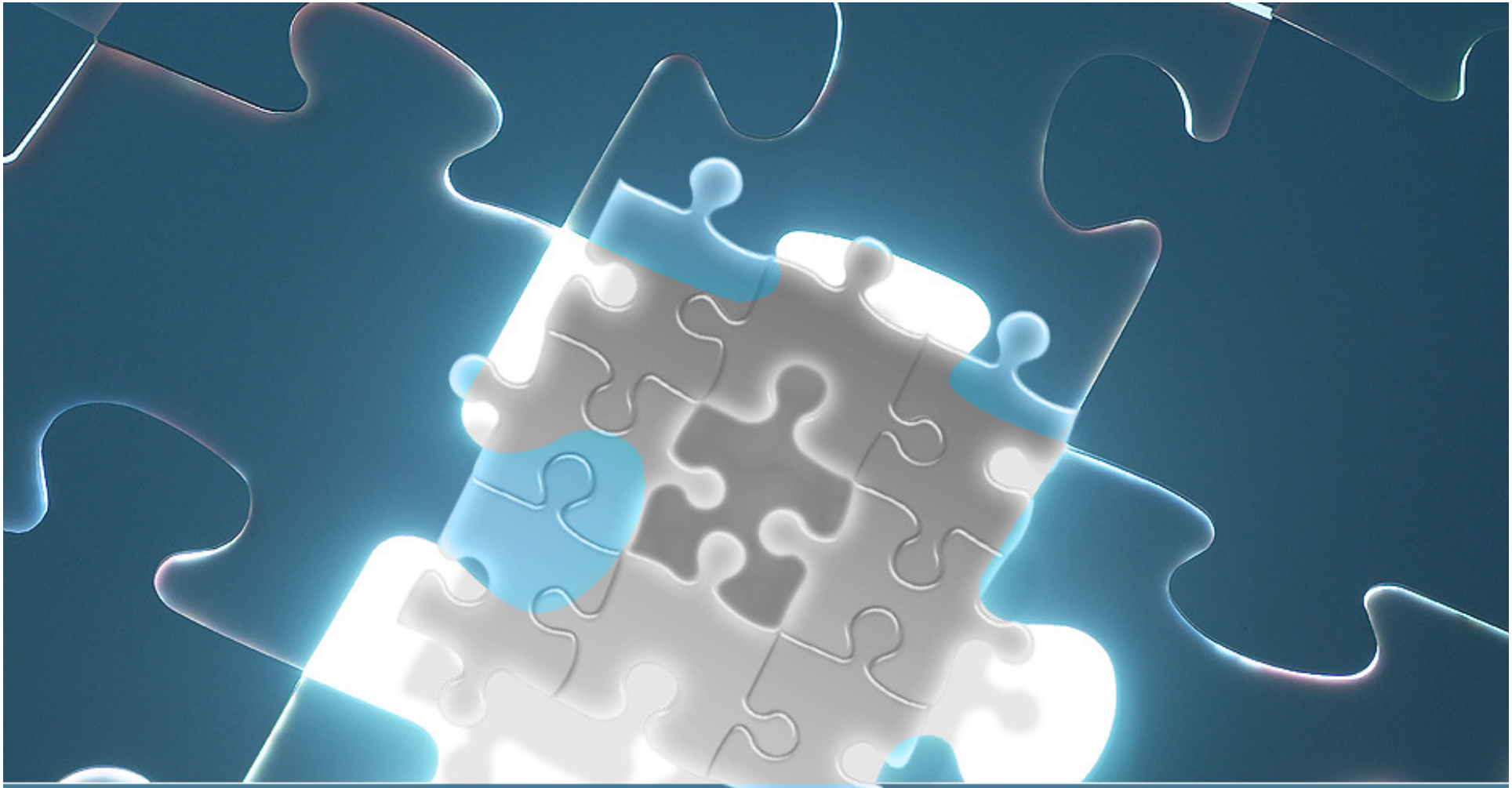


NYS Integrated Justice Portal - Web Services for LEA Interfaces

Background

- NYSPIN (NY Statewide Police Information Network)
- Suite of services for in-state LE and criminal justice users plus agencies nationwide
- Provides access to information on:
  - Wanted, Missing & Unidentified Persons
  - Stolen Property
  - License and Registration
  - Orders of Protection
  - Gang or Terrorist members

Background

- Phased migration from Legacy Mainframe to IJ Portal SOA
- 2009: Move of the message switch back end to service oriented architecture
- 2010: Move from dedicated standalone legacy workstations to browser based portlets
- 2012: Began the migration of LEA's Server-to-Server interfaces to web services
  - Currently these devices are directly connected to NYSP Transitional Gateways
  - Transitional Gateways translate legacy requests before submitting to the Portal

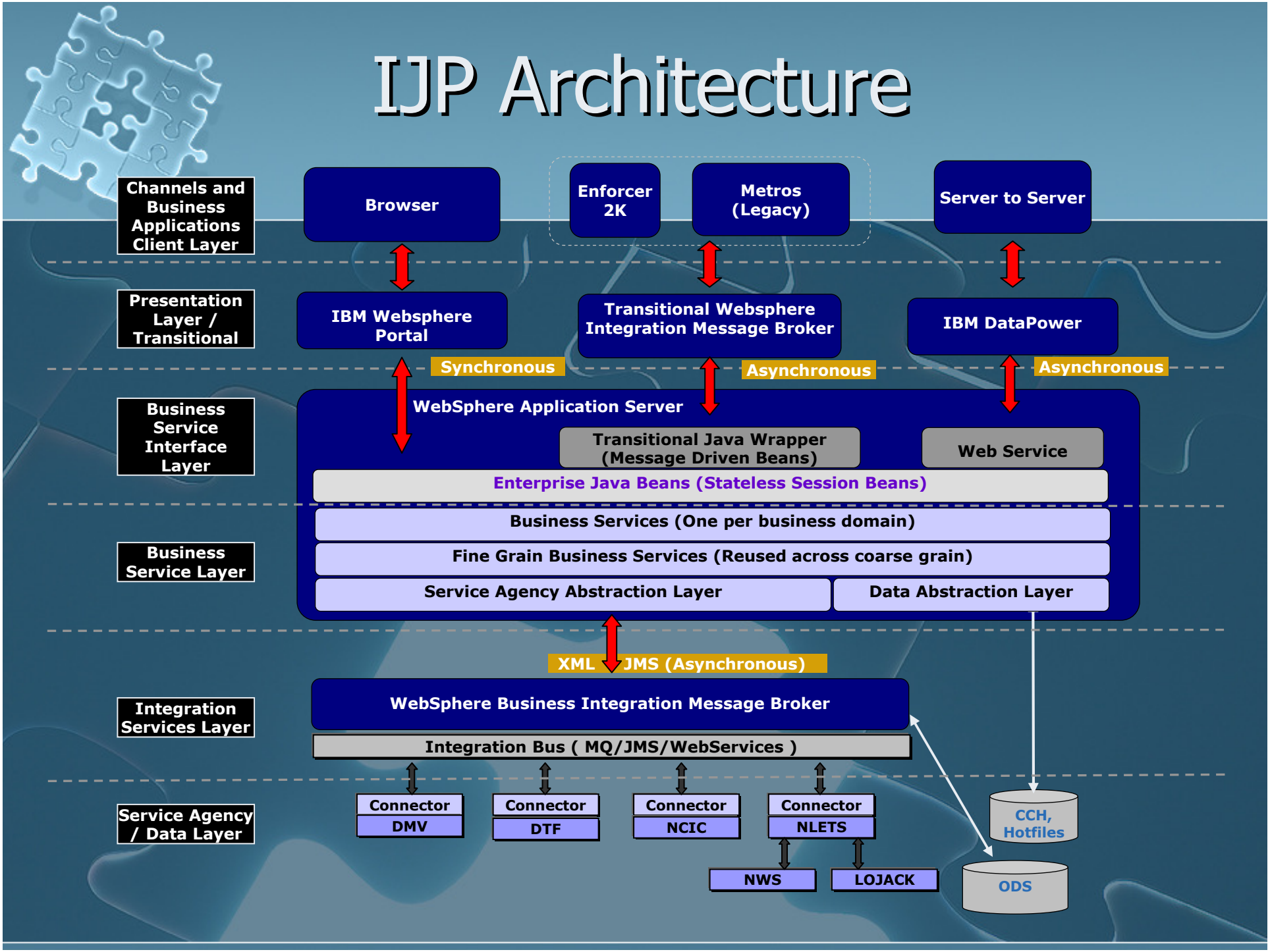
Moving Forward

- Move to Web Services critical
- Network technology supporting dedicated lines must be retired
- Cost of dedicated lines is expensive
- Transitional Gateway – well, it was meant to be "transitional"
- Insufficient resources to support legacy and the IJP at the same time
- Connectivity will be via Internet or OneNet

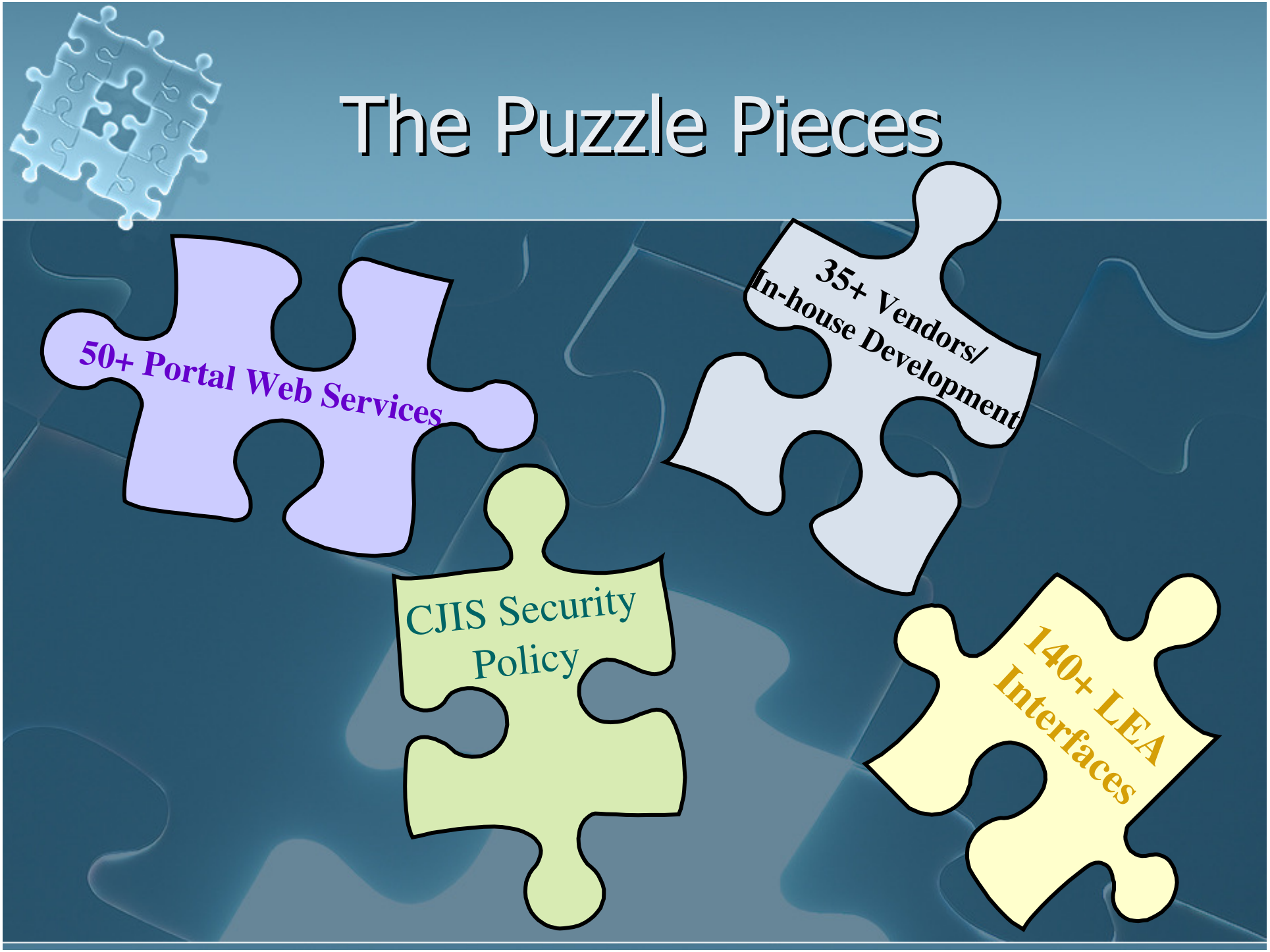
LEA Server-to-Server Interfaces

- CAD, RMS, MDT
- Availability is critical for Officer Safety - 24 hours x 7 days a week
- Consumer is Law Enforcement Officer, Dispatch, Records Management System
- Support for the servers varies from Agency to Agency
  - Law Enforcement
  - Public Safety
  - County IT
  - Vendor

IJP Architecture



The Puzzle Pieces



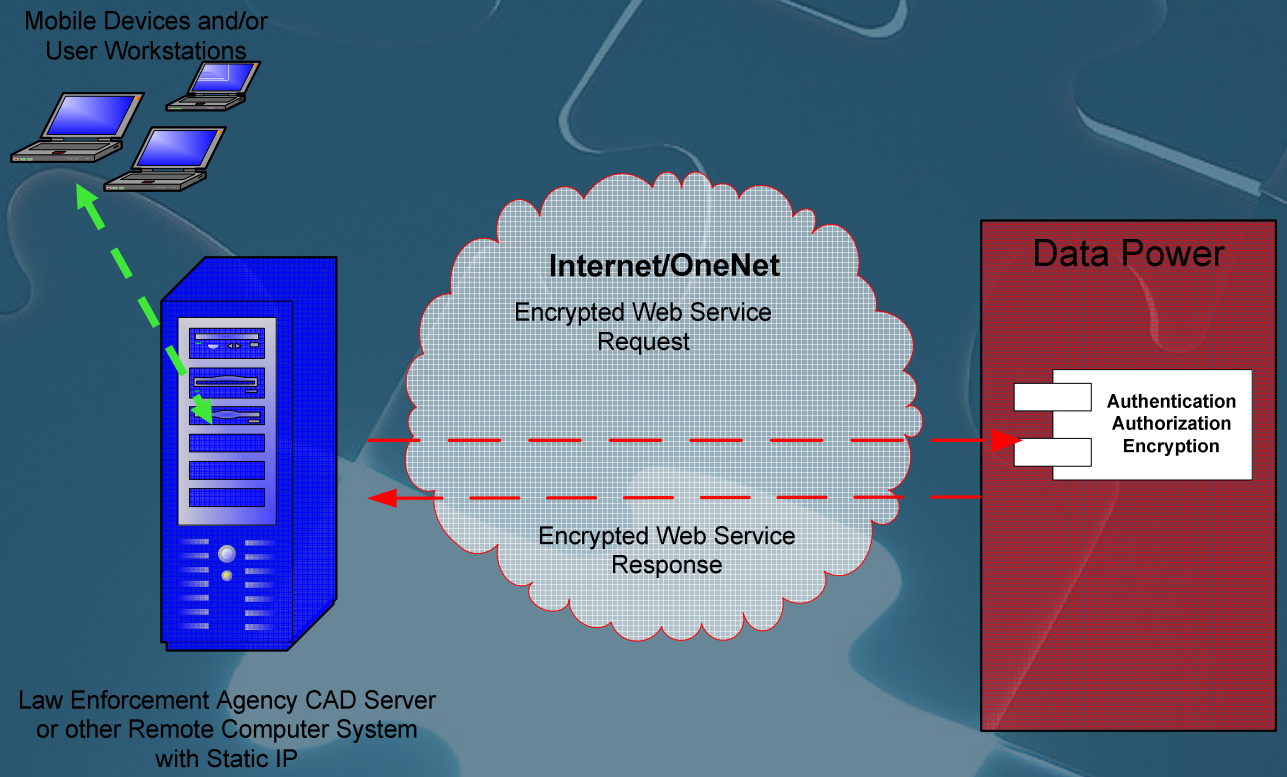
Meeting CJIS Security Policy Requirements

- CJIS Security Policy AA must be met by deadline of 9/30/2013 (CJIS Security Policy 5.1 Section 5.6.2.2.1)
- Policy applies to all NYS public safety agencies that connect directly or indirectly to NCIC (FBI)
- Within New York State all criminal justice agencies obtain CJIS information by accessing the New York State Integrated Justice Portal directly via a browser interface or indirectly via a server interface connection to NCIC

Meeting CJIS Security Policy Requirements

- Responsibility for insuring that these agencies are compliant with the all aspects of the CJIS Security Policy is the function of NYSP & DCJS
- The migration of servers to web services will satisfy the CJIS advanced authentication requirement for the connectivity between the server and IJP
- *Note: It is the responsibility for the agency that maintains the server interface to ensure that the CJIS advanced authentication requirement is satisfied from the remote client application to the server*

LEA Server Interface to IJP



Meeting CJIS Security Policy

- CSO (CJIS Systems Officer) wants *all* applications to meet or exceed the policy requirements
- NYSPIN being first to implement for web services
- Must fit the solution within the defined architecture
- Transport Level encryption used as easier to implement

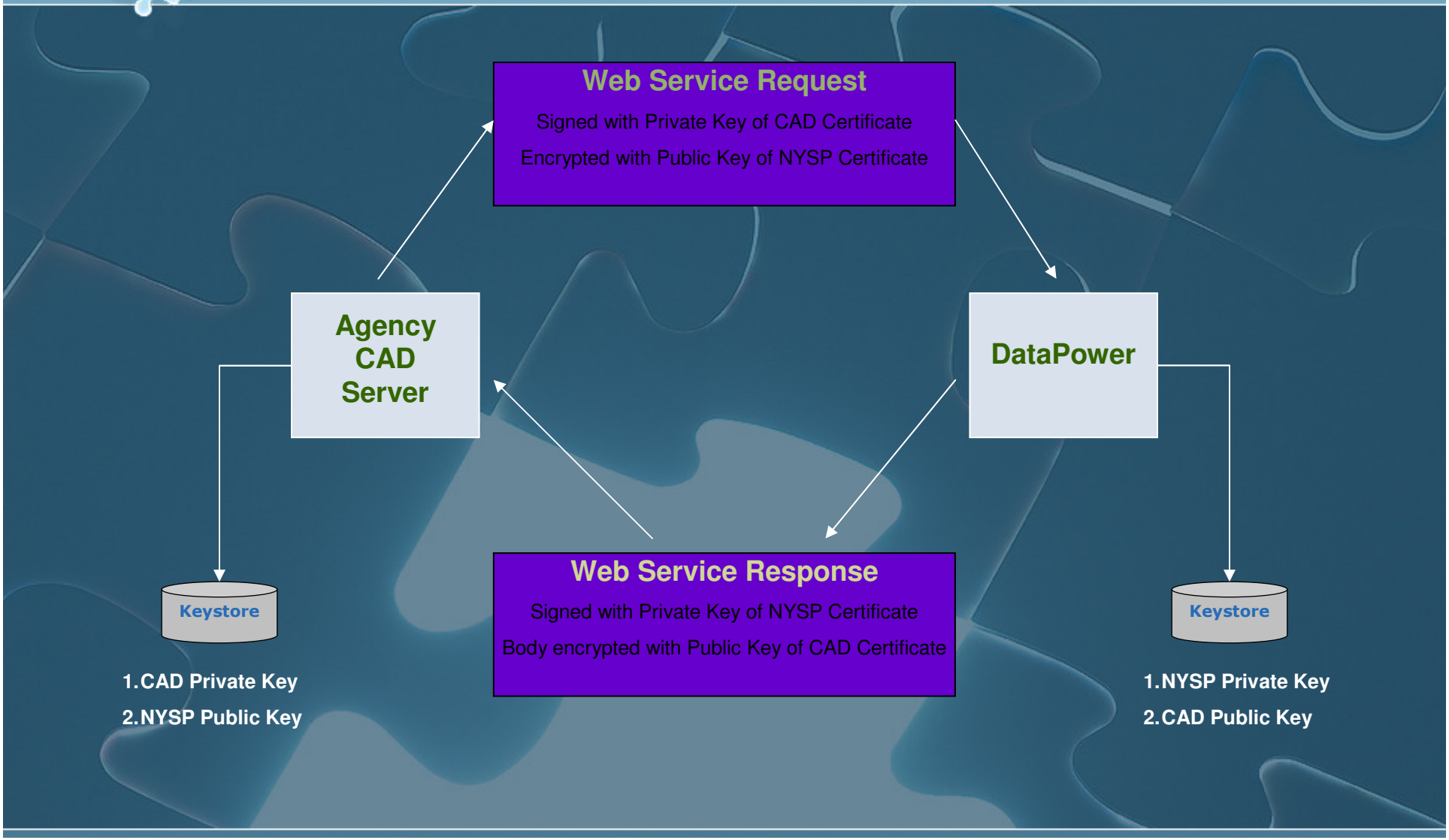
Approach to Satisfy the CJIS Policy Requirements

- Advanced Authentication is based on a match between IJP LDAP userid and password assigned to the LEA server plus valid certificate
- Certificates will be issued by Certificate Authority
- Encryption must be minimum 128 bit and certified to meet FIPS 140-2 standard
- NYSP purchasing for all LEA servers

Symantec Managed PKI

- PKI addresses the multiple hop scenario which occurs on the internet and OneNet
- Trusted Source
- Covers any incident for $250,000
- Supports multiple domains
  - NYENET.STATE.US
  - NY.GOV
- Portal Interface for Certificate/Key Management
  - Configurable by Customer
  - *Timely alerts for requests and expiration of Certs*

Managed PKI (Pubic Key Infrastructure)



Challenges with Certificates

- For Agencies using OneNet for connectivity, the state owns the domain and can issue the certificate without a "Domain Rights Confirmation"
- For Agencies using ISP, NYS does not own the domains
- Results in Symantec "whois" search and request to use domain for generating certificate

Domain Rights Confirmation

Dear Symantec,

I, _____,

Confirm that I am the administrative contact for the domain, *domain.name.com*, which is registered to *Domainowner*. NYS Office for Technology has the right to use, or has full control of the domain(s), *domain.name.com*.

Registrant acknowledges that it has granted Certificate Applicant the right to use the Domain in connection with its business and as a *common name in the Digital Certificate request referenced above* and any subsequent and/or additional certificates obtained by the Certificate Applicant during the validity of the above referenced certificate.

Domain Rights Confirmation

- Domain owner may not know about LEA project
- LEA personnel may not know the domain owner
- This is limited to generating certificate for use in the IJP server interface
- NYSP can *only* use for this purpose within the Managed PKI portal

Meet in the Middle

- NYSP did not want to pass the cost of the certificates to the Agencies
- Centralization of Certificate administration to prevent loss of service and ensures compliance
- Need implicit trust between LEAs, their IT support and Integrated Justice

CJIS Policy and IT Resources

- CJIS Security Policy requires all resources that have access to CJIS data to be:
  - Fingerprinted
  - Background check
  - CJIS Policy Training
- Includes Agency Resources, IT Resources and Vendors
- Next CJIS Audit is September 2013!

Contact Information

- For questions concerning the CJIS Security Policy:

  Capt. William Tatun
  Phone: 518-457-6501
  Email: William.Tatun@troopers.ny.gov

- For questions concerning CJIS online policy training:

  Tech Sgt. Douglas Johnstone
  Phone: 518-457-8822
  Email: Douglas.Johnstone@troopers.ny.gov

- For questions concerning the web services conversion:

  Glori Ekberg
  Phone: 518-485-7777
  Email: Glori.Ekberg@troopers.ny.gov

  Mike Morrill
  Phone: 518-485-8332
  Email: Mike.Morrill@troopers.ny.gov

Thank you!