Policy Driven Data Centric Information Sharing and Safeguarding

Data Centric Security for Structured Data Environments

Tide Sprint Briefing

DCS - CWIX 2018

M. Abramson - CAN

Presentation Assumptions

- DCS CWIX 2018 was focused on the sharing of structured data elements using STANAG 4559
- Many of the slides can be discussed for an hour or more – we have 20 minutes for all the slides
- I would be pleased to answer any questions at the end of the brief or between sessions
- Additional Information Exchange Framework presentation tomorrow @

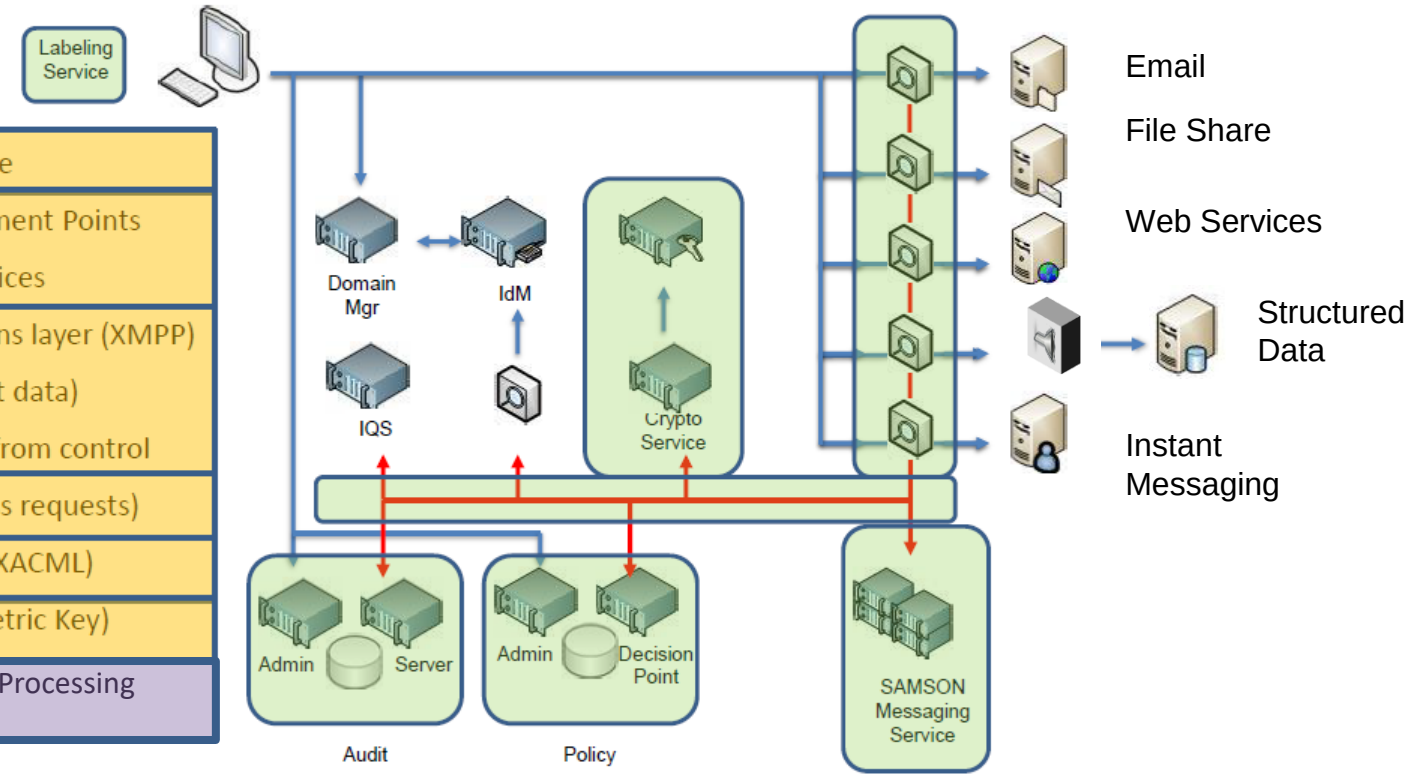
Many Terms For the Same Set of Requirements

- Data Centric Security (DCS) is an approach that applies security measures directly to the data based on the sensitivity of that data
  - An additional security layer in a defense in depth strategy – targeting the data elements
  - An architecture that augments and relies on exiting security services
  - An approach for automating electronic Information Sharing Agreements (eISA)
  - An implementation that enforces user defined policy
- Information Sharing and Safeguarding (ISS)
  - Balancing the responsibility to share and the requirement to protect
  - Focus on the Information/data (Object level protection)
  - Apply the safeguards appropriate to the sensitivity of the data
  - Sharing and safeguarding are inseparable concepts
- Data Exchange v Data Protection
  - inseparable/mutually Reinforcing
  - Effective safeguarding generates trust
  - Trust produces a willingness to share
- Interoperability
  - The Right Information, to the Right Person, at the Right Time

Extending 2016 DCS Capability

(Focus on Unstructured Data)

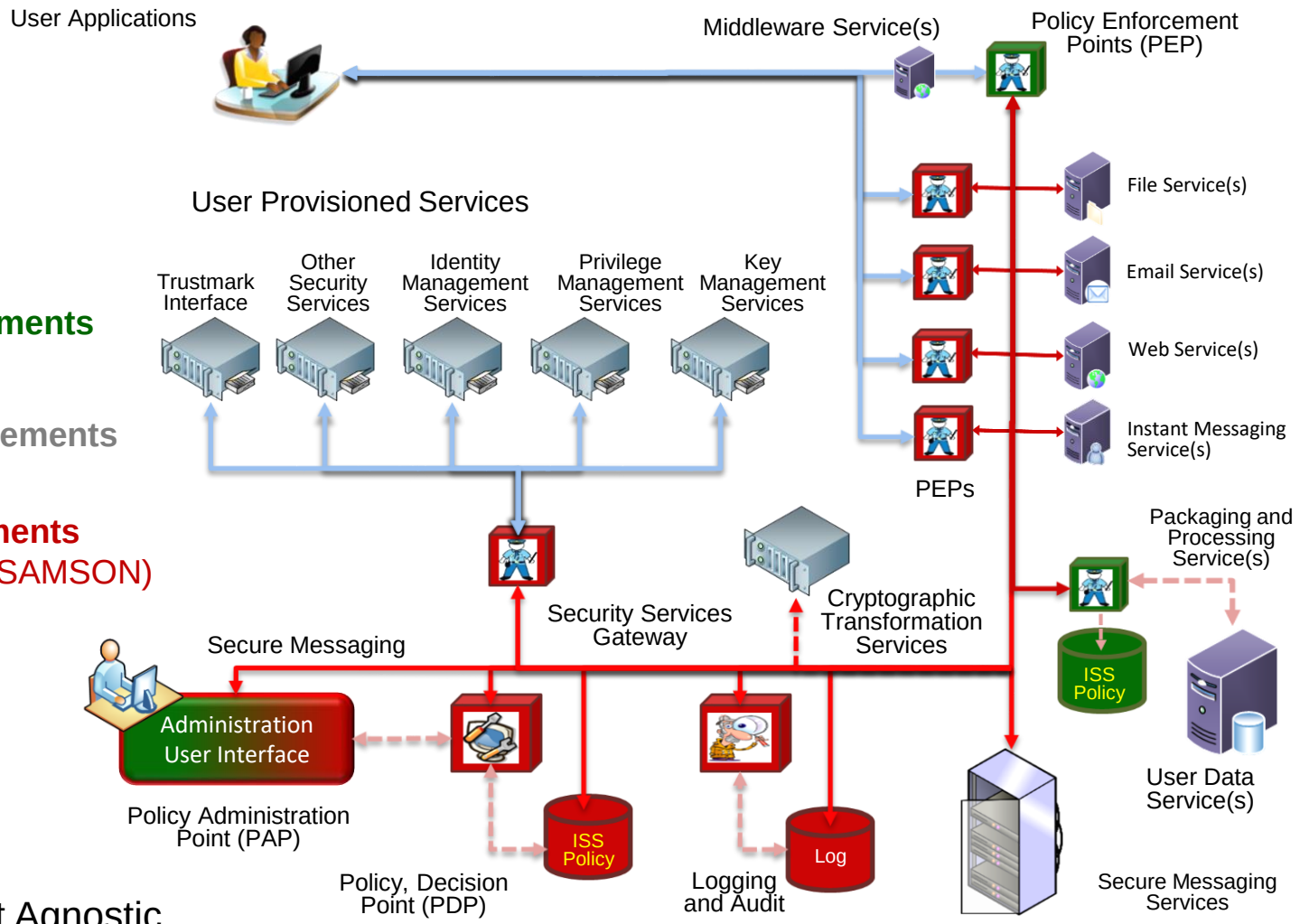
1. Labeling Service
2. Policy Enforcement Points in front of services
3. Communications layer (XMPP) to services (not data) separate data from control
4. Audit (all access requests)
5. Policy engine (XACML)
6. Crypto (Symmetric Key)
7. Packaging and Processing Services (PPS)



DCS in the IEF Reference Architecture (IEF-RA)

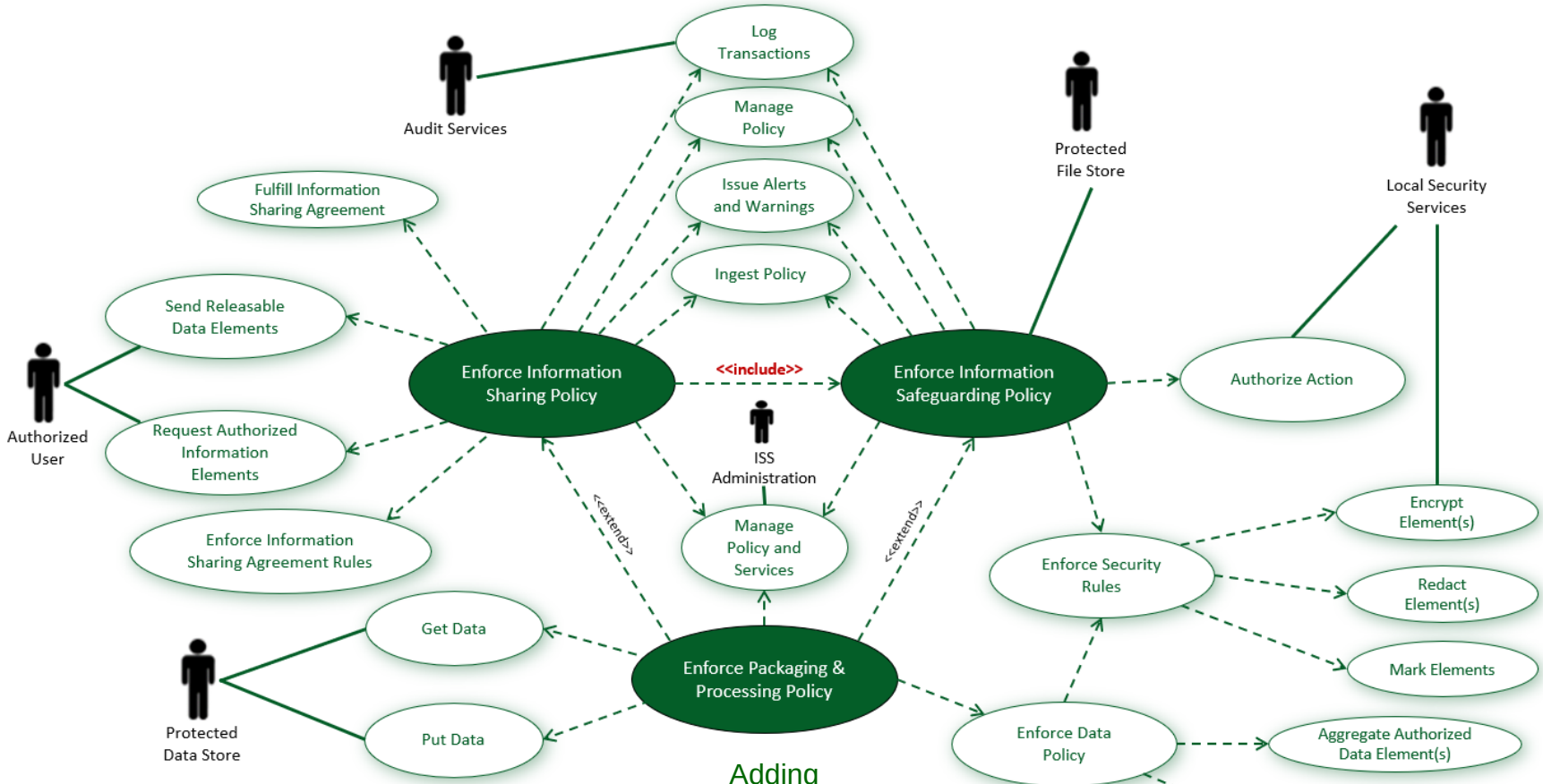
(http://www.omg.org/spec/IEF-RA/)

1. **IEF-RA: Defined Elements**
   (Structured Data)
2. **User Provisioned Elements**
3. **IEF RA Defined Elements**
   (Unstructured Data - SAMSON)



- Open Standards
- Vendor Neutral
- Data Environment Agnostic

IEF Use Case for Structured Messaging



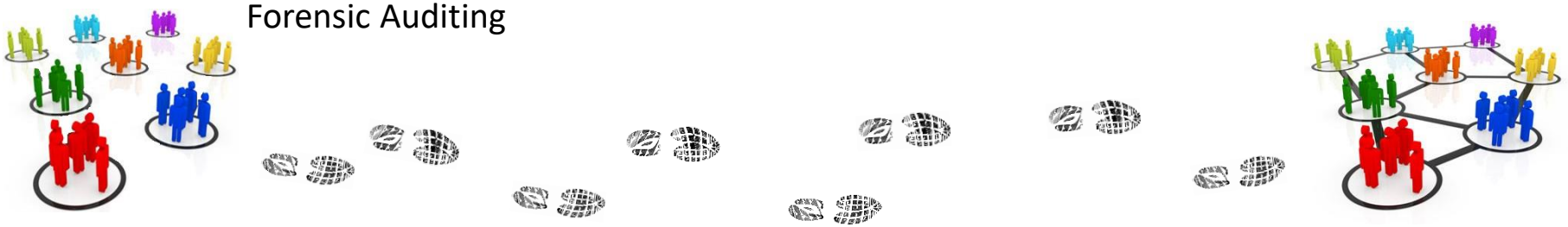
The Problem with Structured Data

- Exchanges are generated in real-time at machine speeds limiting the ability of users to mediate individual exchanges
- A single change in data can results the need to generate multiple messages that:
  - Address different information needs
  - Provided to recipients with different authorizations to access that data
  - Using different communication channels and protocols
- Each message needs to be tagged/labeled based on it its content (also at machine speeds) in order to enable traditional security services
- Actual content is only known when an exchange is generated
- No good plan (design) survives first contact with operations

Crossing the Data Divide

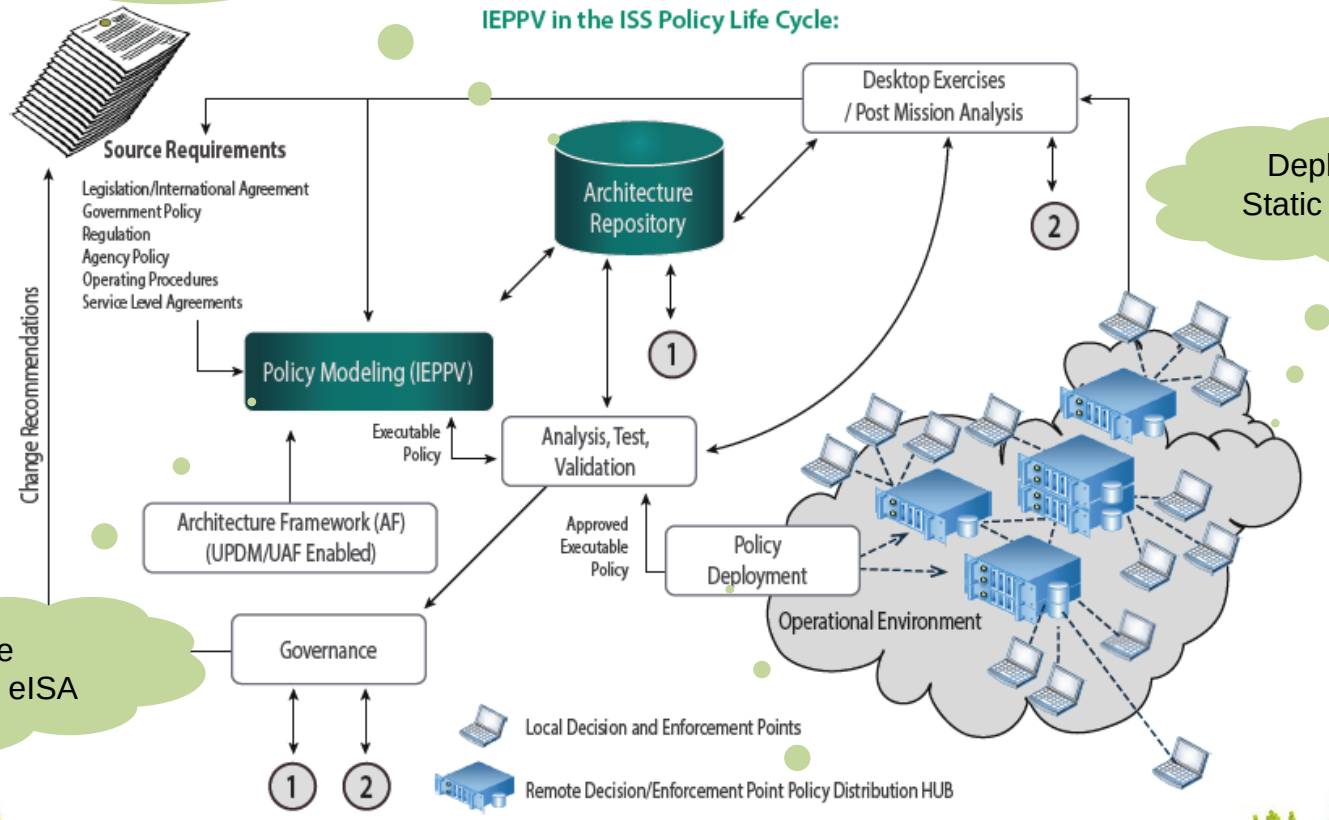
Responsibility to Share

- Separate Operational, Information Management/Security, and Technology concerns
- Separate lifecycles for:
  - Software Services
  - Information Sharing policies (rules and constraints)
- Runtime control over:
  - Active polices
  - Software configurations
- Development practices and runtime logging that enable:
  - Design Auditing
  - Real-time Monitoring / Alerts and Warnings
  - Forensic Auditing



Interoperability by Design

Full eISA documented and linked to applications, systems, platforms, networks, operations and missions through Architecture

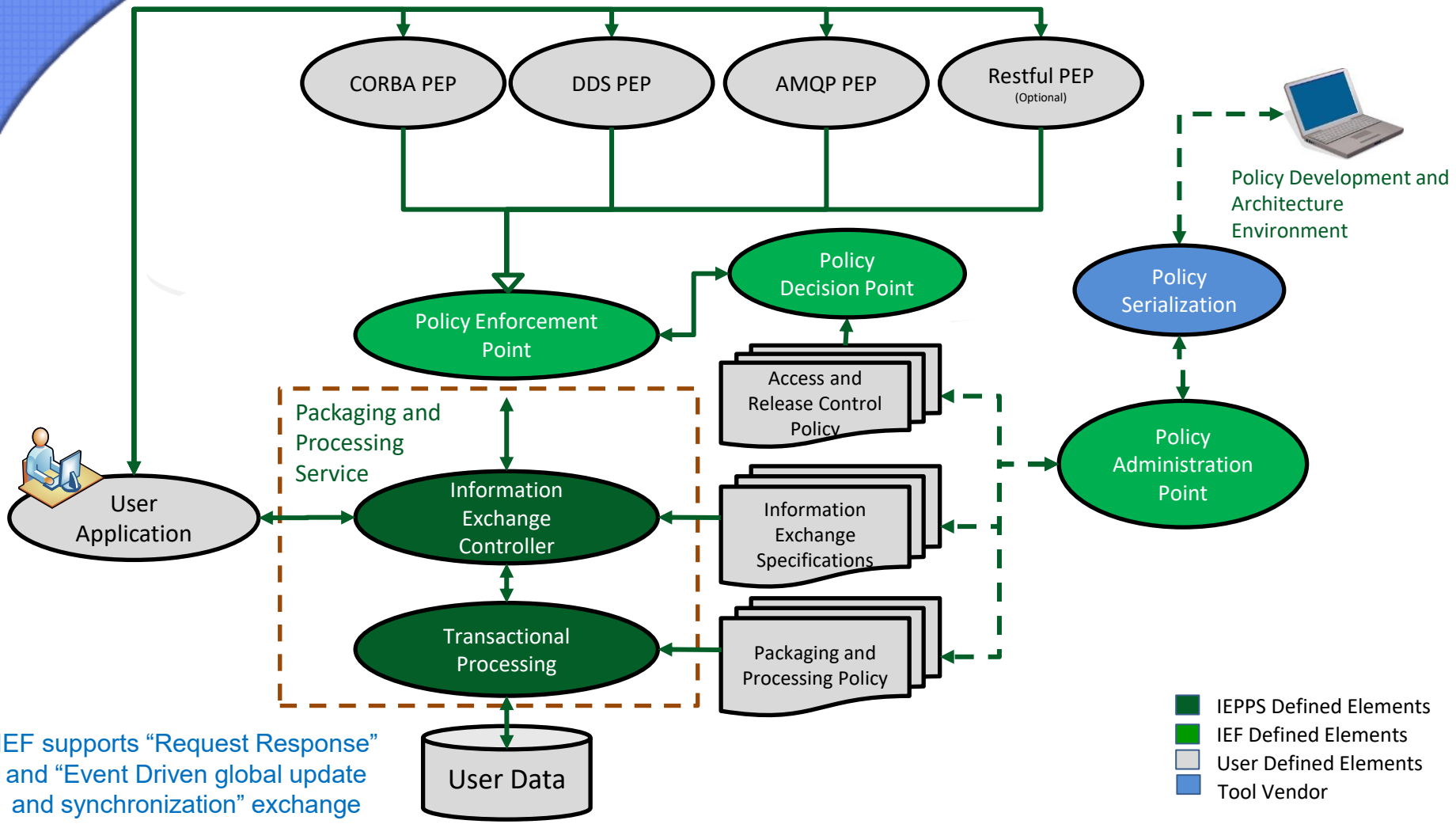


Deployed or Static Networks

Executable elements of an eISA

Policy and configurations deployed as signed data

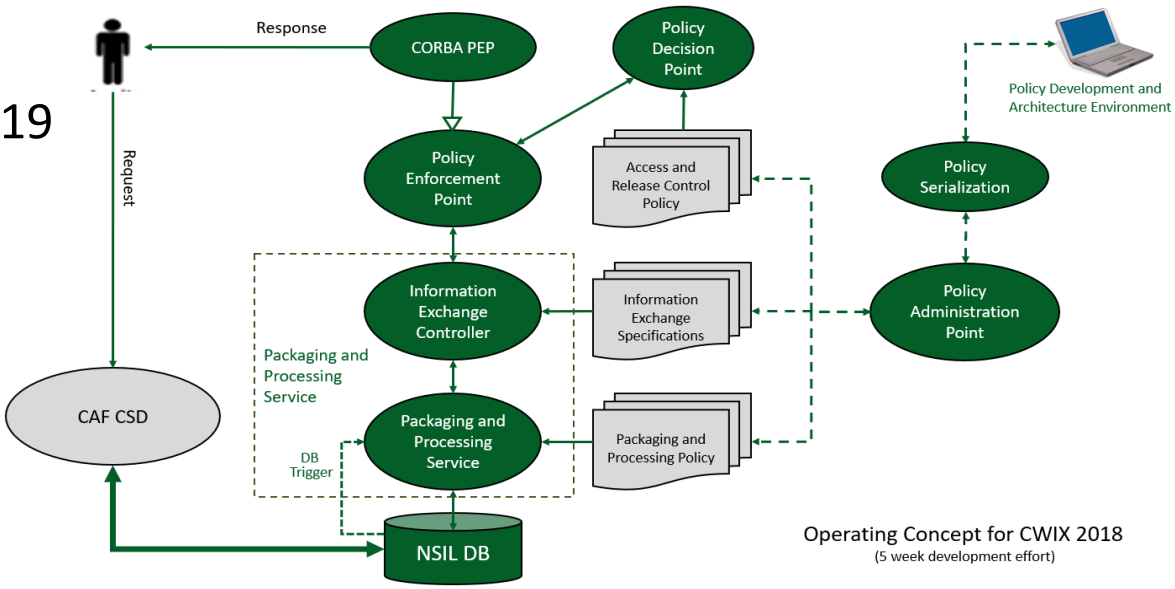
Configuration for Structured Data



IEF supports "Request Response" and "Event Driven global update and synchronization" exchange paradigms

CWIX 2018 Objectives

- Initial Integration of IEF and CAF CSD
- Develop STANAG 4559 Policy Model
- Execute basic interoperability testing
- Engage with testing partners
- Learn about CWIX
- Explore opportunities for 2019



CWIX 2018 Achievements

~30 person-weeks of development effort – from a cold start

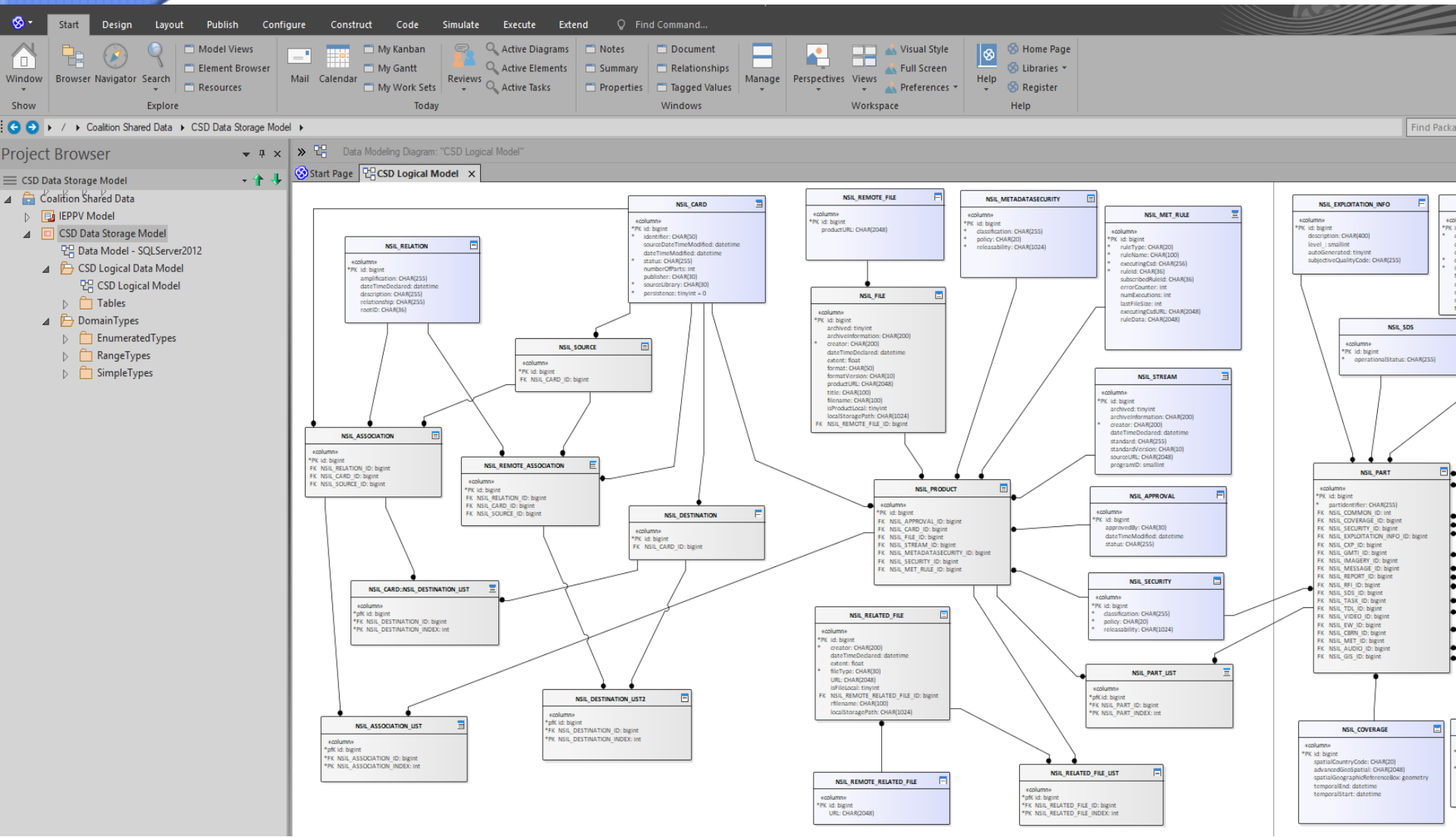
- Initial Integration of CAF-CSD Application with IEF
- Initial testing of IEF / CAF-CSD within the CWIX Environment
- Developed a much better understanding of CWIX
- Developed a much better understanding of the CSD/NSIL Requirements and related standards

MAJOR

- Partially tested executable policy model for STANAG 4559 views that could be integrated into NAF
- Policy model took days to develop – not months developing and testing interface code

NATO Standard ISR Library (NSIL)

Reverse Engineered Database Schema

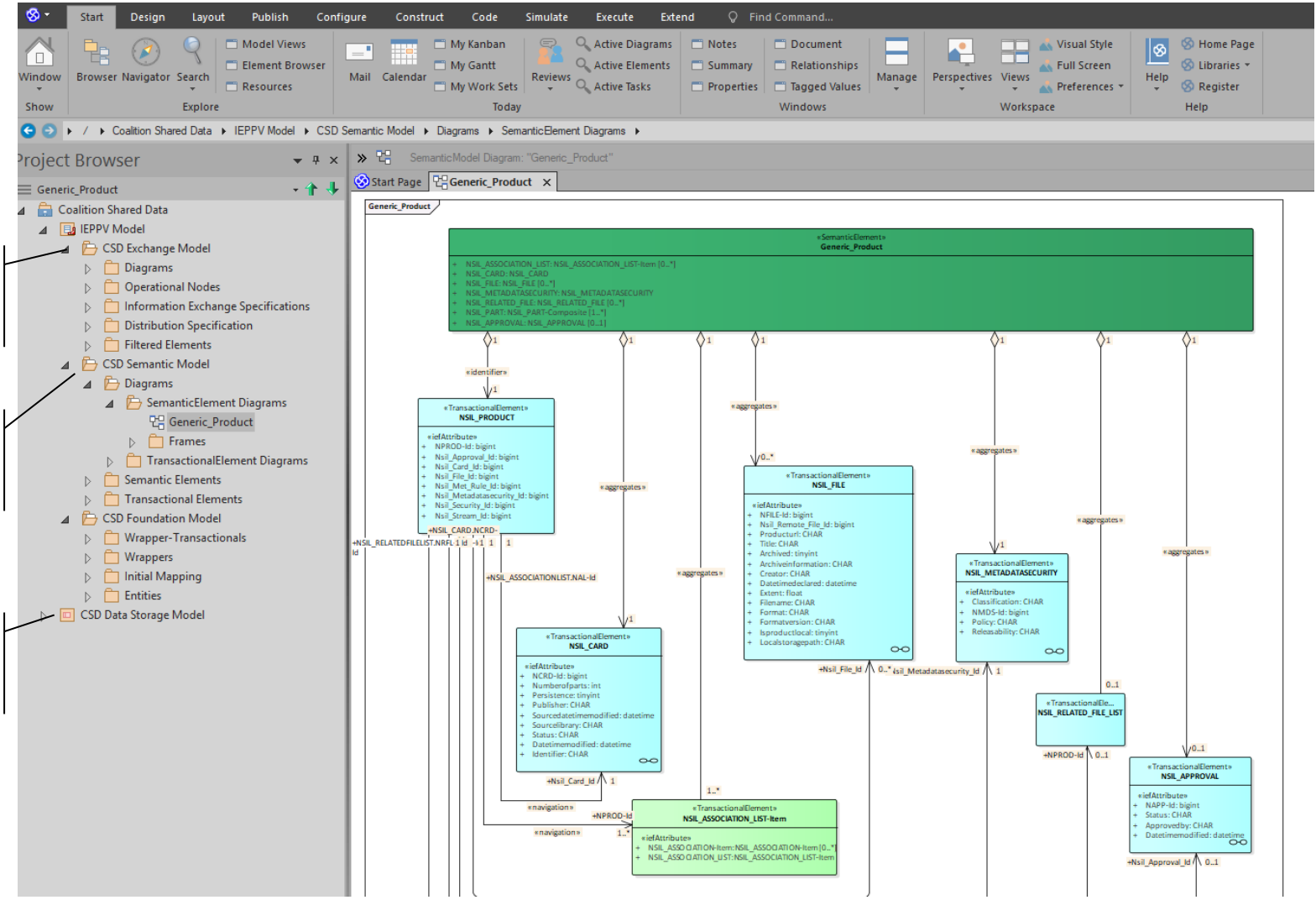


Architected/Documented eISA

eISA in an executable form

Exchange Semantics

Linked to its Data Source



Basic transactional

NSIL Part Tailored for NSIL_Report

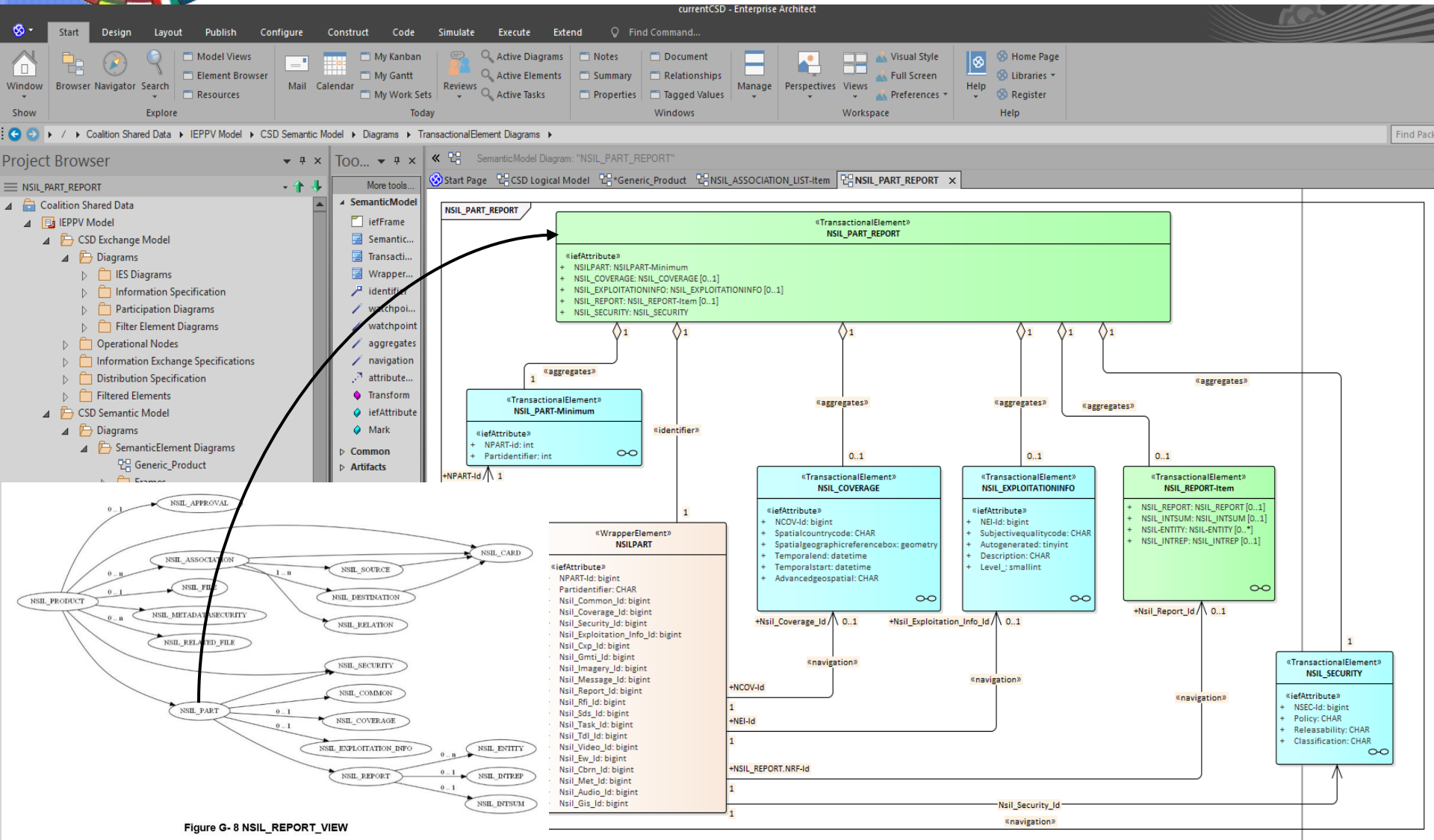


Figure G- 8 NSIL_REPORT_VIEW

Summary of Lessons Learned

- Would have been better to focus on NSIL DB Synchronization than Data Requests given time and resource constraints
- Time to absorb 100s of pages of documentation pointing to 10s of specifications (1000s of pages) was a significant hurdle
- Significant time/effort was expended reverse engineering documents into an architecture model that supported the Model Based Systems Engineering (MBSE) ASMG employs
- Reference architectures for DCS and the CSD in a Machine-readable form would have streamlined efforts
- Only having the developer at CWIX during testing impacted knowledge transfer – having an Architect

Recommendations

- More opportunity to work with partners between June and June
  - Share Architecture
  - Testing between events
  - Focus on new use cases and demonstration during the event
- Scenario based testing vs discrete tests
  - Role based test data available for implementation teams to use
  - Reference implementation for remote testing
  - Scenario used to demonstrate working capability (repeatedly)
- Look to Model based Systems Engineering (MBSE) to automate interoperability standards
  - Architecture (metadata driven) vs document driven data/interface standards
  - Tools for operators (Analysts vs Programmers) to tailor capability to mission requirements

CWIX 2019 Target

- Seeking partners for 2019 testing
  - Coalition Shared Data Environment
  - NATO Core Data Framework (NCDF)
  - MIP
  - Combination of the above or Other
- Seeking an Environment
  - Multiple Exchange Schemas (/Semantics)
  - Distinct need to separate data based on security, Caveat or QoS
  - Inclusion of STANAGS 4774 and 4778 for tagging and labeling
- To support evaluation:
  - Example Models for CSD, MIEM, CAP and (limited MIP Model) available upon request (Requirement Sparx EA or a Tool that imports Sparx's Files)
  - Community version of the IEF elements (Slide 10) will be ready for release CWIX 2019 – Testing Partners will be provided license to experimentation and evaluation

Mike Abramson

Special Adviser to Public Safety Canada in Information Sharing and Safeguarding (ISS) and Open Interoperability Standards

Co-Chair C4I DTF at OMG

Chair IEF WG at OMG

President Advanced Systems Management Group (ASMG) Ltd.

265 Carling Ave, Suite 630, Ottawa, Ontario, K1S2E1

Fax: 613-231-2556

Phone: 613-567-7097 x222

Email: abramson@asmg-ltd.com