

# TESTBED-15

## Data-Centric Security



Digital  
Signatures &  
Encryption



OGC API-  
Features &  
Proxies



STANAG

# API Support

- Security classification (additional metadata fields)
- Representation of data source/origin
- Tampering
- Implementations that ensure “all-time” encryption



SECURED  
CONTAINER



NATO STANAG  
4778, 4774



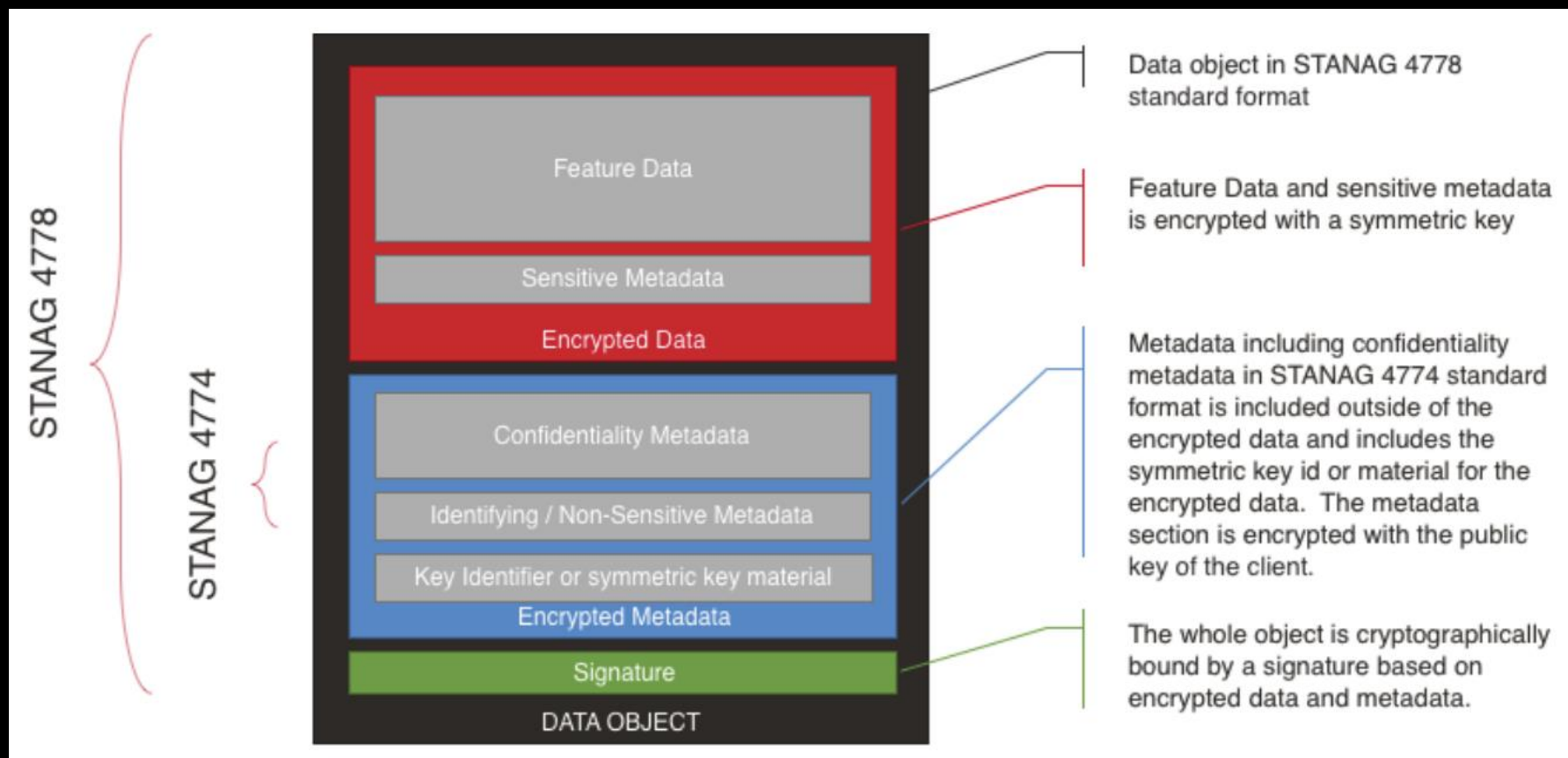
FEATURE  
COLLECTION

STANAG 4778: Information on Standard Metadata Binding

STANAG 4774: Confidentiality Metadata Label Syntax

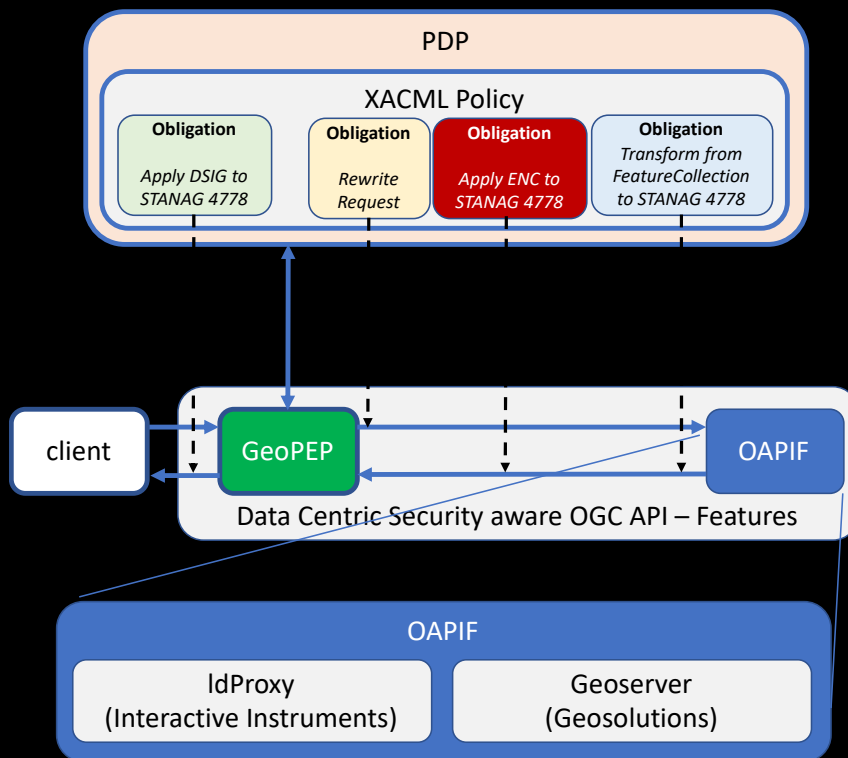
permit the sharing of sensitive information between allies

# STANAG 4778 and 4774

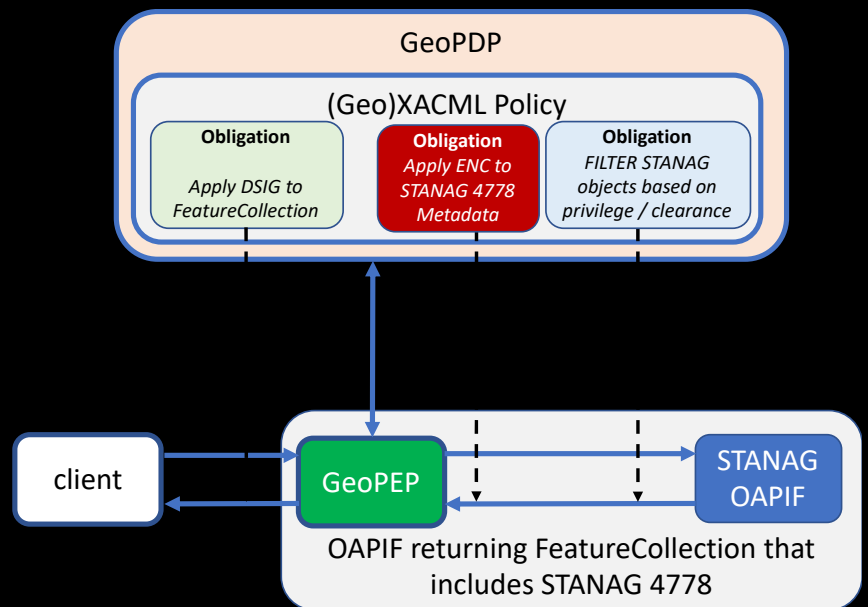


# Implementation Alternatives

- From a “vanilla” FeatureCollection to DCS



- DCS Objects inside a FeatureCollection



# TB15 DCS Demonstration

## Users and Features

- Demo users and their fictitious clearance

Username	Clearance
jane	Top secret
bob	secret
alice	classified
joe	unclassified

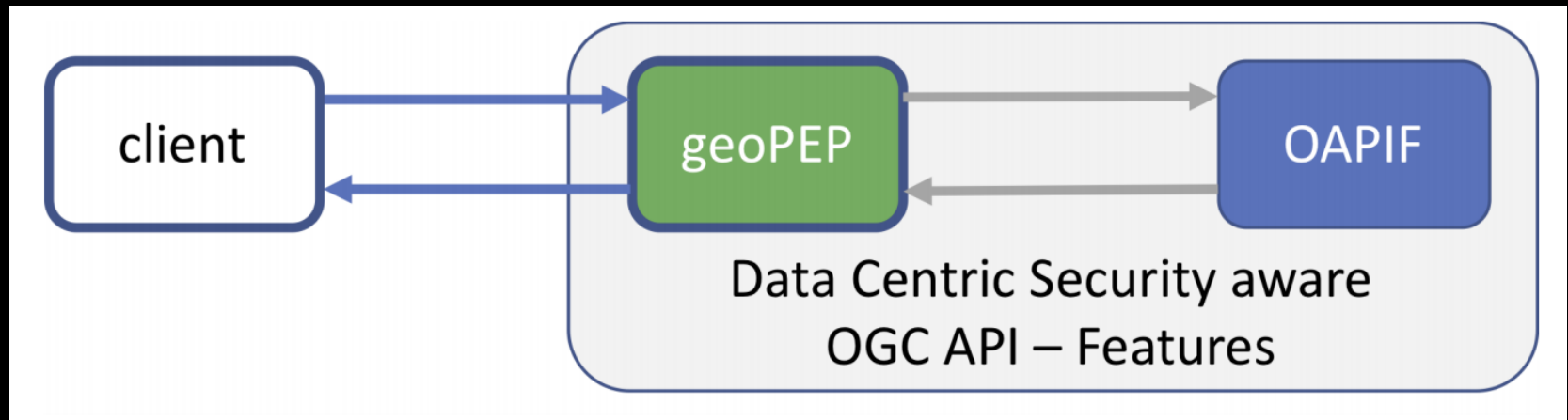
+

- Feature types and their fictitious classification

Feature type	Classification
poly_landmarks	top secret
poi	secret
tiger_roads	classified
states	unclassified

=

Username	Action	Feature type
jane	read	poly_landmarks, poi, tiger_roads, states
bob	read	poi, tiger_roads, states
alice	read	tiger_roads
joe	read	states



User	States	Roads	PoIs	Landmarks
Jane	YES	YES	YES	YES
Bob	YES	YES	YES	NO
Alice	YES	YES	NO	NO
Joe	YES	NO	NO	NO



# Disaster Access Policy for Jane

- Jane has the clearance to fetch feature type **tiger\_roads**
- If Jane submits a geo-location, her clearance is overwritten and the returned features are inside the (disaster) area.
- Jane outside (disaster) area before 12:00UTC
- Jane inside (disaster) area before 12:00UTC

Manhattan (NY) roads

Filter

« < 1 2 3 4 5 > »

**tiger\_roads.1**

id	tiger_roads.1
CFCC	A41
NAME	Washington Sq W

**tiger\_roads.2**

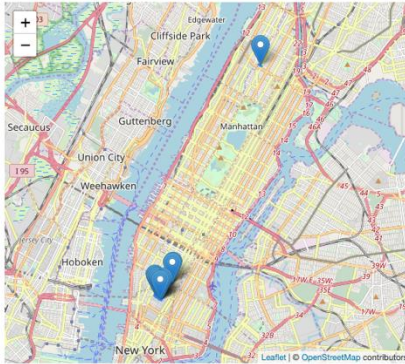
id	tiger_roads.2
CFCC	A41
NAME	W 126th St

**tiger\_roads.3**

id	tiger_roads.3
CFCC	A41
NAME	Union Sq W

**tiger\_roads.4**

id	tiger_roads.4
CFCC	A41
NAME	Union Sq W



[https://ogc.secure-dimensions.com/rest/services/DCS/collections/tiger\\_roads/items?f=stanag&access\\_token=](https://ogc.secure-dimensions.com/rest/services/DCS/collections/tiger_roads/items?f=stanag&access_token=)

Manhattan (NY) roads

Filter

« < 1 2 3 4 5 > »

**tiger\_roads.1**

id	tiger_roads.1
CFCC	A41
NAME	Washington Sq W

**tiger\_roads.3**

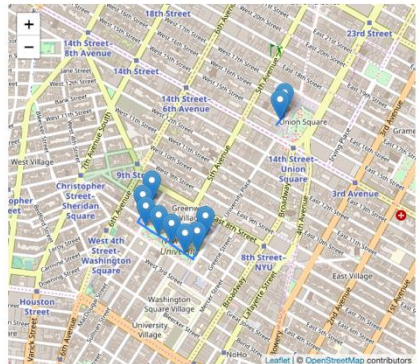
id	tiger_roads.3
CFCC	A41
NAME	Union Sq W

**tiger\_roads.4**

id	tiger_roads.4
CFCC	A41
NAME	Union Sq W

**tiger\_roads.5**

id	tiger_roads.5
CFCC	A41
NAME	Washington Sq E



[https://ogc.secure-dimensions.com/rest/services/DCS/collections/tiger\\_roads/items?f=stanag&subjectlocation=CRS=EPSG:4326;POINT\(40.75%20-74.00\)&access\\_token=](https://ogc.secure-dimensions.com/rest/services/DCS/collections/tiger_roads/items?f=stanag&subjectlocation=CRS=EPSG:4326;POINT(40.75%20-74.00)&access_token=)



# Spatio-Temporal Overrides

- Joe has no clearance to fetch feature type tiger\_roads
- If Joe submits a geo-location, his clearance is overwritten and the returned features are inside the (disaster) area.
- Joe has no clearance to fetch feature type tiger\_roads
- If Joe's request is outside the (disaster) time window, his clearance is *\*not\** overwritten. Geolocation has no effect!

	Outside Geometry	Inside Geometry
Before time condition	Alt 1	Alt 1
During time condition	Alt 1	STO
After time condition	Alt 1	Alt 1

# Encountered Challenges

- No support for NATO standards in current code lists
- STANAG 4778 is a container format (encrypted + metadata)
  - Two encodings to be specified
    - Container
    - Content of container
- STANAG 4778 does not handle mix of Data Centric Security formats
  - Collections with combined DCS formats not supported
- Key management
  - API not aware of any keys (even public keys!)
    - API cannot act on data, but only forward (no filtering etc. possible)
- Digital signatures missing in current *WFS FeatureCollection* scheme (CR #614)

# Results

- 3 scenarios demonstrated
- Recommendations for
  - Digital signatures
  - Media types for STANAGs
- Future work:
  - Key management
  - Sophisticated authentication and authorization schemes
  - How to search an encrypted database?
  - Consider TDF (Trusted Data Format) and flavors
- Future Standards Program work:
  - Container formats (multi-encodings)
  - Digital signatures