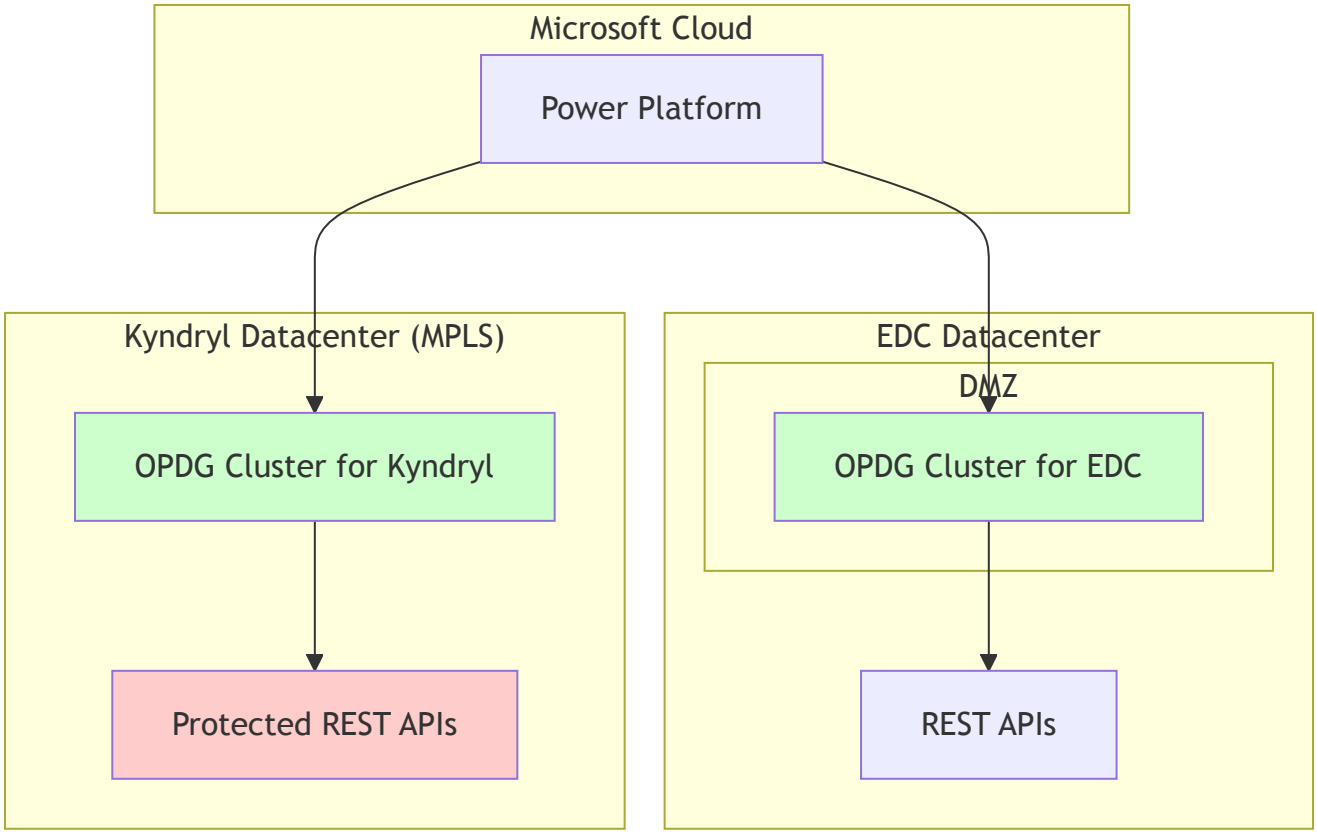
Overview

This document defines the mandatory configuration requirements for enabling Power Platform access to REST APIs hosted in Elections Canada's two datacenters using the On-Premises Data Gateway (OPDG). After security analysis, we recommend implementing **Option 1: Dedicated OPDG in Kyndryl Datacenter** as the most secure approach for Protected data, while maintaining other options as viable alternatives based on specific requirements.

The recommended implementation will:

1. Deploy separate OPDG clusters in both datacenters to maximize security isolation
2. Utilize the DMZ in EDC with two non-domain joined servers in a high-availability cluster running the OPDG for EDC APIs
3. Deploy a dedicated OPDG cluster in Kyndryl datacenter for direct, secure access to Protected APIs
4. Eliminate cross-datacenter traffic for Protected data, ensuring maximum security for sensitive information
5. Provide secure, isolated access paths from Power Platform to each datacenter



Current Environment

- The DMZ VMs in EDC are not domain-joined (by design for machine-to-machine workflows)
- DMZ servers have firewall configurations that allow communication with EDC but not currently with Kyndryl
- Kyndryl datacenter enforces stricter security requirements for Protected data and does not expose APIs to the cloud
- While an MPLS connection exists between EDC and Kyndryl, introducing additional network hops and cross-datacenter traffic increases the security risk profile

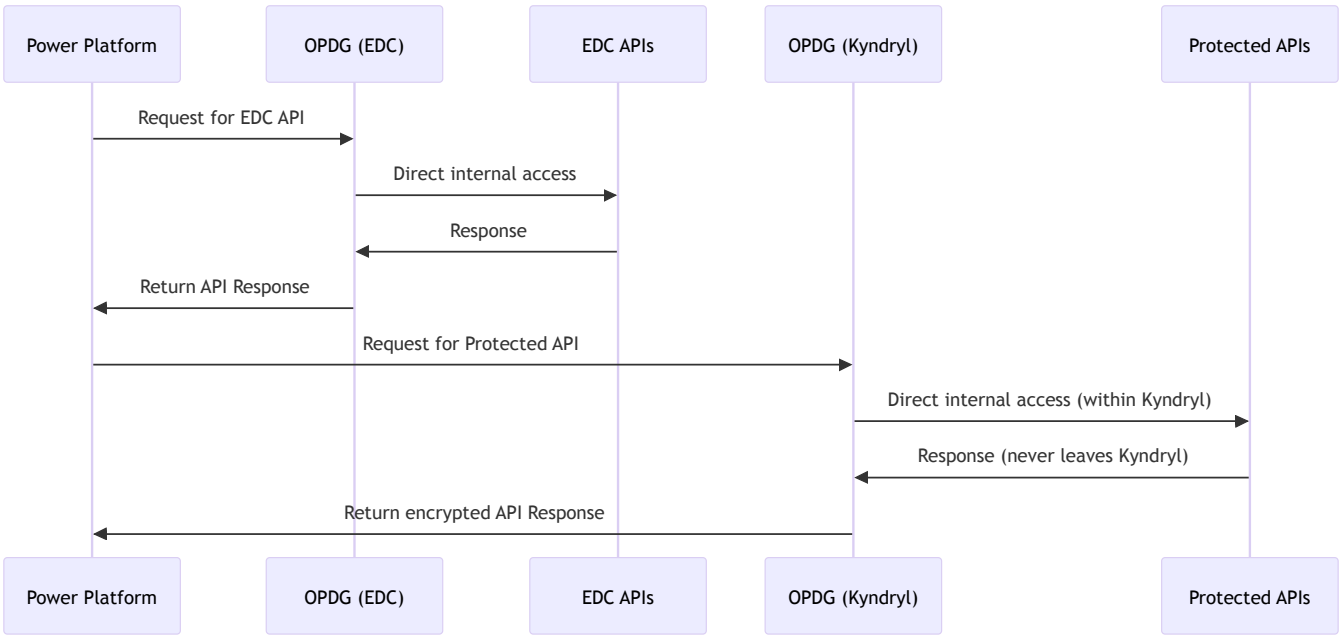
Strategic Solution: Option 1 - Dedicated OPDG in Kyndryl Datacenter

This option implements separate OPDG clusters in each datacenter, creating fully isolated security boundaries and eliminating cross-datacenter traffic for Protected data.

1. Security Architecture

Deploying a dedicated OPDG cluster directly in Kyndryl provides several critical security advantages:

1. **Elimination of Cross-Datacenter Traffic**: Protected data never traverses between datacenters, even over MPLS
    - Each OPDG cluster only accesses APIs within its own datacenter
    - API responses remain within their security boundary until encrypted for cloud transit
    - Reduces attack surface by eliminating additional network hops
2. **Security Boundary Isolation**: Creates distinct security zones for different data sensitivity levels
    - EDC OPDG cluster handles standard data classification APIs
    - Kyndryl OPDG cluster exclusively handles Protected data
    - Physical and logical separation enforces security classification boundaries
3. **Reduced Attack Surface**: Minimizes potential vectors for compromise
    - No firewall rule exceptions needed between datacenters for API traffic
    - Eliminates potential for lateral movement between environments
    - Each gateway only requires access to APIs within its own datacenter
4. **Enhanced Monitoring and Auditing**: Provides clear visibility into Protected data access
    - Dedicated logging for all Protected API access
    - Simplified audit trails with clear demarcation of Protected data flows
    - Streamlined compliance reporting for Protected requirements



2. OPDG Cluster Implementation

1. **EDC OPDG Cluster Deployment**:
   - Deploy OPDG on non-domain joined DMZ servers in EDC
   - Configure gateway in high-availability cluster mode
   - Register with Elections Canada's Power Platform tenant
   - Restrict API access to only EDC endpoints
2. **Kyndryl OPDG Cluster Deployment**:
   - Deploy two new servers in Kyndryl datacenter for OPDG
   - Configure as separate high-availability cluster
   - Register with same Elections Canada Power Platform tenant but as distinct gateway
   - Implement enhanced security controls for Protected compliance:
     - Hardware security modules for key storage
     - Enhanced monitoring and logging
     - Network-level isolation from other systems
3. **Power Platform Configuration**:
   - Configure separate connections for each gateway cluster
   - Implement clear naming conventions distinguishing Protected connections
   - Apply appropriate data loss prevention policies to each connection

3. Enhanced Security Implementation for Protected

1. **Network Security Architecture**:
    - Implement dedicated network segment in Kyndryl for OPDG servers
    - Apply defense-in-depth with multiple security layers:
        - Network segmentation with dedicated firewall zones
        - Host-based firewalls on OPDG servers
        - Network intrusion detection/prevention systems
        - Encrypted communications at all levels
    - Restrict outbound connectivity to only Azure Service Bus endpoints
2. **Comprehensive Authentication Security**:
    - Implement certificate-based authentication for all API access
    - Deploy hardware security modules (HSMs) for key protection
    - Enforce mutual TLS (mTLS) for all API communications
    - Implement just-in-time access controls for administrative functions
    - Utilize Microsoft Entra ID (formerly Azure AD) for robust authentication
3. **Advanced Monitoring and Incident Response**:
    - Deploy behavioral analytics monitoring for OPDG traffic
    - Implement real-time alerts for anomalous access patterns
    - Conduct regular penetration testing against both gateways
    - Establish dedicated incident response procedures for Protected data
    - Configure comprehensive audit logging with tamper-proof storage

Alternative Options for Consideration

While Option 1 provides maximum security, the following alternatives remain viable based on specific requirements:

Option 2: Network Configuration Between EDC and Kyndryl Datacenters

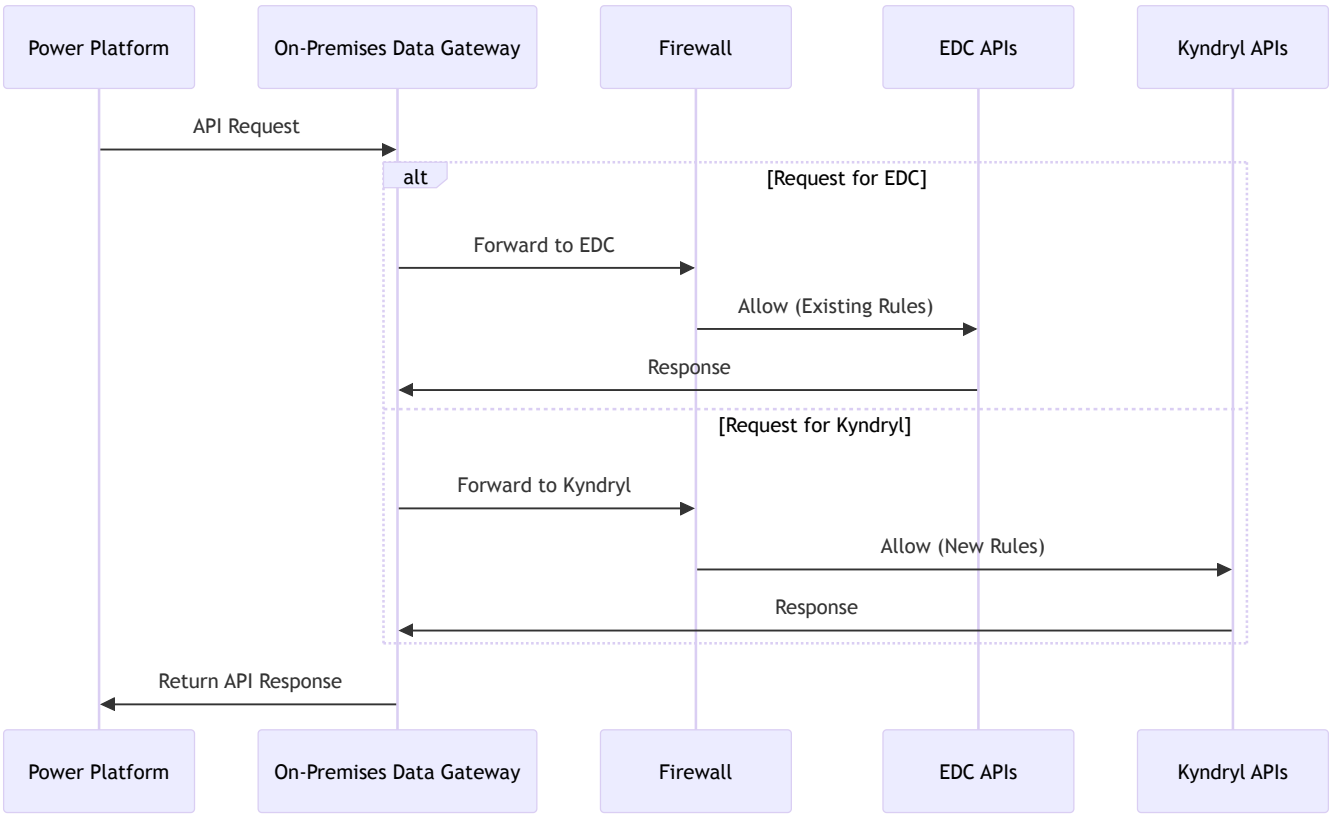
This option implements secure network connectivity between EDC and Kyndryl to allow the OPDG in EDC's DMZ to access the APIs in Kyndryl.

Key Security Limitations:

- Protected data must traverse between datacenters (even if over MPLS)
- Additional network hops increase attack surface
- More complex firewall rule management required

- More challenging to audit and monitor Protected data flows

1. **Firewall Rule Implementation**:
   - Configure rules for required ports (443 for HTTPS)
   - Restrict access to only necessary IP addresses and ports
   - Enable comprehensive logging for all traffic
2. **Network Routing Implementation**:
   - Utilize the existing logical network link between EDC and Kyndryl
   - Configure routing tables on DMZ servers for API requests to Kyndryl



Option 3: API Proxy in EDC Datacenter

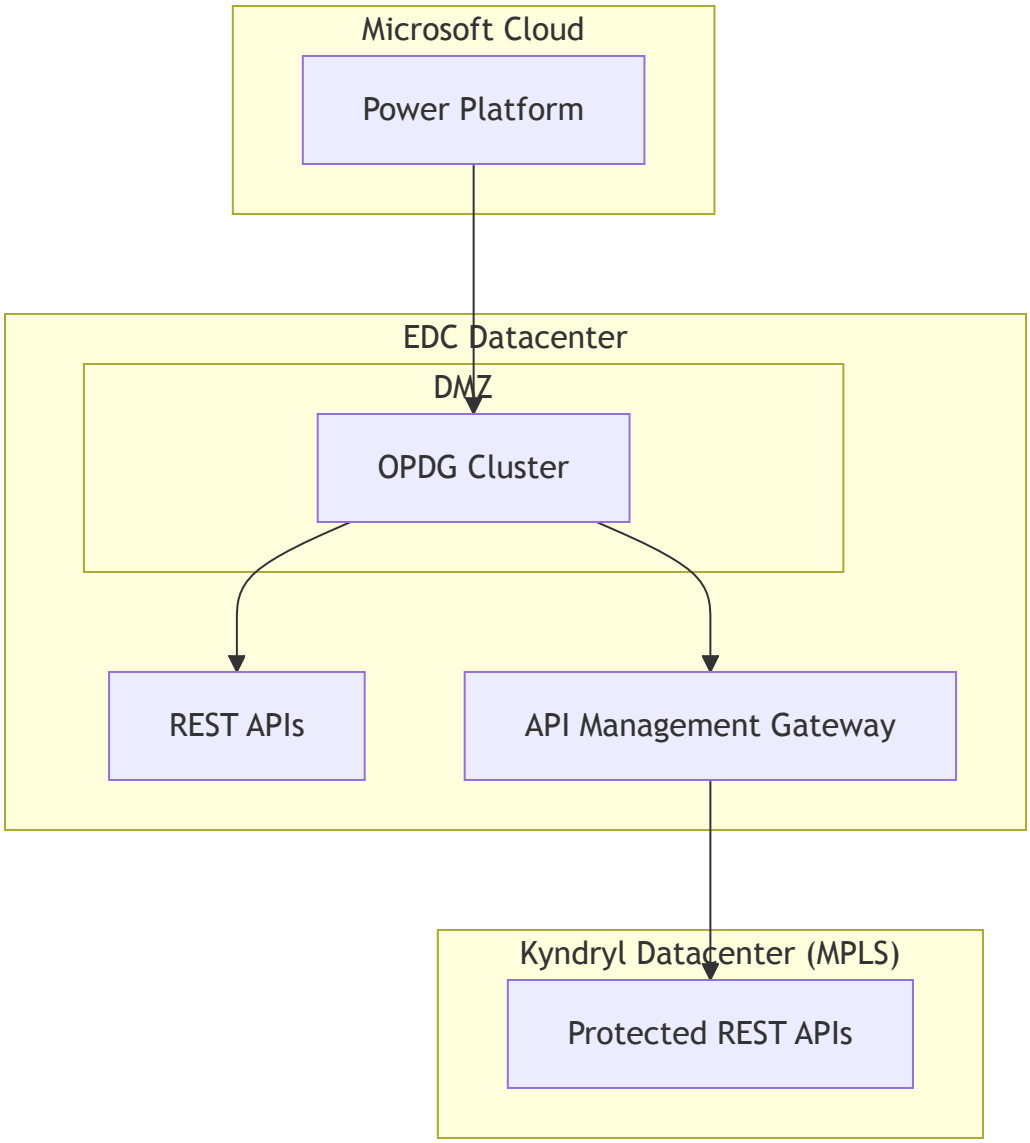
This option deploys an enterprise API management gateway in the EDC datacenter to handle and secure all requests to Kyndryl.

Key Security Limitations:

- Protected data still traverses between datacenters
- Additional processing layer increases complexity
- API proxy becomes a potential single point of failure
- More complex error handling and troubleshooting

Strategic Benefits:

- Consolidated API governance and monitoring
- Enhanced security controls with API request inspection
- Consistent API policy enforcement



Option 4: GC Cloud Virtual Network Implementation

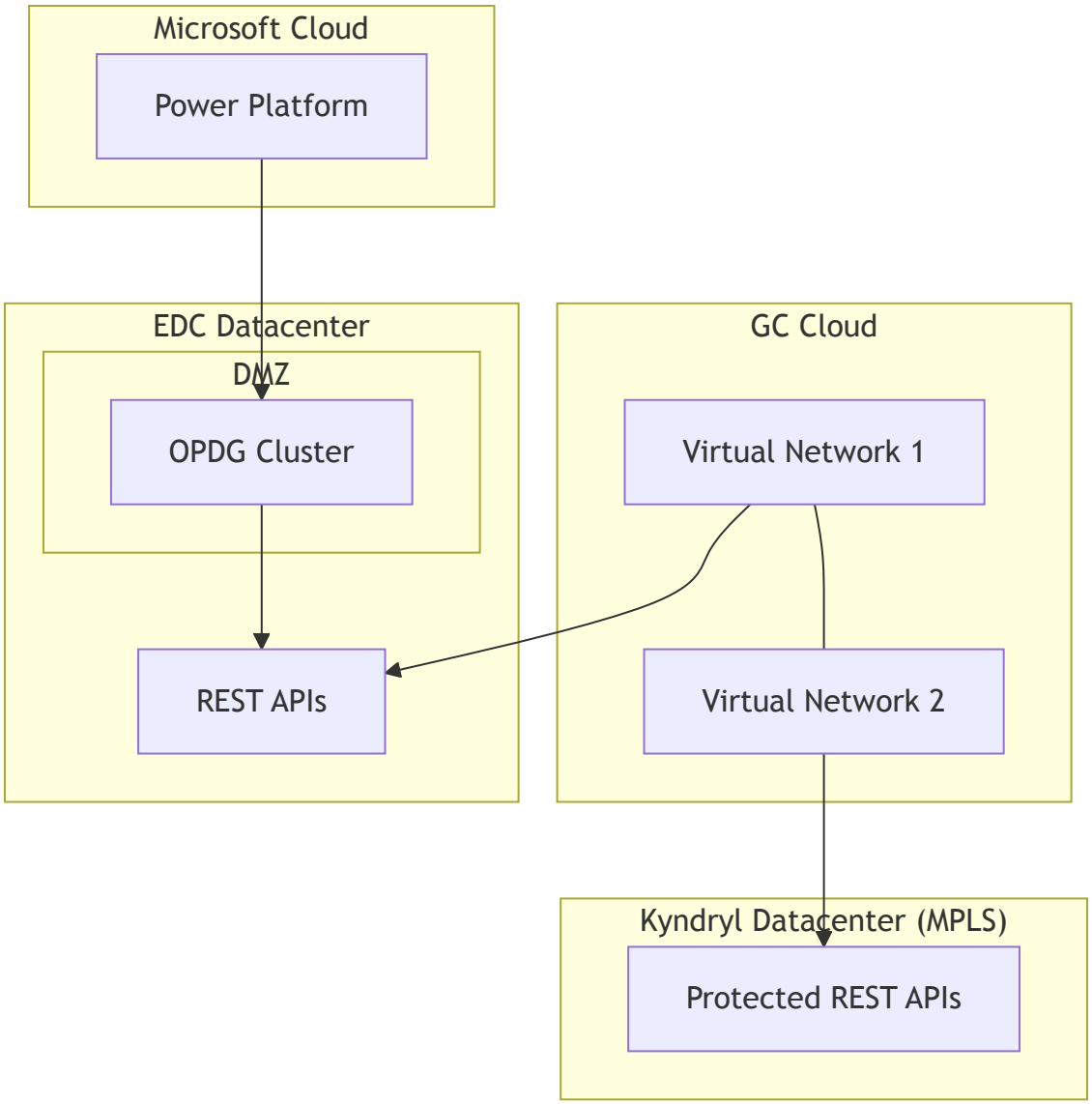
This option leverages GC Cloud Virtual Network capabilities to establish secure connectivity between environments while maintaining Protected compliance.

Key Security Considerations:

- Requires GC Cloud network implementation
- May introduce cloud-based processing of Protected data
- Requires additional architectural components

Strategic Benefits:

- Secure connectivity with end-to-end encryption
- Leverages GC-approved cloud networking capabilities
- Infrastructure-as-code deployment



Governance and Operational Management

Service Management Framework

1. **Service Ownership**:
   - Designate separate EC IT staff for each OPDG environment
   - Establish clear roles and responsibilities matrix
   - Define escalation paths for incidents

2. **Change Management**:
    - Implement formal change control processes for gateway configuration changes
    - Require security review for new API connections
    - Maintain configuration documentation
3. **Capacity Planning**:
    - Monitor gateway performance metrics
    - Plan for scaling based on usage patterns
    - Establish thresholds for resource utilization

Standard Operating Procedures

1. **Installation and Updates**:
    - Schedule coordinated but separate gateway updates
    - Test updates in non-production environment first
    - Maintain version control for gateway configurations
    - Document rollback procedures
2. **User Access Management**:
    - Implement quarterly access reviews
    - Enforce separation of duties
    - Document onboarding/offboarding procedures
3. **Incident Response**:
    - Define response procedures for gateway outages
    - Establish communication plans
    - Conduct regular tabletop exercises
4. **New Connection Onboarding Process**:
    - Implement formal request process for new connections
    - Require security assessment for all new APIs
    - Mandate business justification documentation
    - Enforce testing in lower environments before production

BUILD BOOK ANNEXES

ANNEX A: OPDG Cluster Installation and Configuration

A.1 Prerequisites for Both Environments

- Windows Server 2019/2022 VMs (two in each datacenter)
- Each VM with minimum 8 cores, 16GB RAM, 100GB storage
- .NET Framework 4.7.2 or later installed
- TLS 1.2 or later enabled
- Outbound connectivity to Azure Service Bus endpoints
- Service accounts with appropriate permissions

A.2 EDC OPDG Installation Process

1. Download the latest On-Premises Data Gateway installer from Microsoft
2. On first server, run installer as administrator
3. Select "New gateway installation" option
4. Authenticate with Elections Canada Power Platform admin account
5. Set a recovery key and store in secure location
6. Name the gateway "EC-OPDG-EDC-Primary"
7. Complete installation and verification
8. On second server, run installer as administrator
9. Select "Register a gateway on this computer"
10. Authenticate with same Elections Canada Power Platform admin account
11. Enter the recovery key from primary installation
12. Select the existing gateway name to join the cluster
13. Complete installation and verification

A.3 Kyndryl OPDG Installation Process for Protected

1. Provision two dedicated servers in Kyndryl datacenter in secure network segment
2. Configure servers with enhanced security hardening:
    - Disable unnecessary services and ports
    - Implement application whitelisting
    - Apply security baselines exceeding CIS Level 2

    - Deploy advanced endpoint protection
    - Enable comprehensive audit logging
3. Download the latest On-Premises Data Gateway installer
4. On first server, run installer as administrator
5. Select "New gateway installation" option (not joining existing cluster)
6. Authenticate with Elections Canada Power Platform admin account
7. Set a unique recovery key and store in secure location (different from EDC)
8. Name the gateway "EC-OPDG-KYNDRYL-PB-Primary"
9. Complete installation and verification
10. On second server, run installer as administrator
11. Select "Register a gateway on this computer"
12. Enter the recovery key from Kyndryl primary installation
13. Select the Kyndryl gateway name to join the cluster
14. Complete installation and verification

A.4 Gateway Security Configuration

1. **General Security Measures (Both Environments)**:
    - Configure Windows Firewall on all servers
    - Implement OPDG monitoring using Windows Performance Counters
    - Configure gateway service to run under dedicated service account
    - Set appropriate service recovery options
    - Configure backup of gateway encryption keys
2. **Enhanced Security for Kyndryl OPDG (Protected)**:
    - Implement hardware security modules for encryption key storage
    - Configure enhanced audit logging for all gateway operations
    - Deploy host-based intrusion detection system
    - Implement network traffic filtering at multiple layers
    - Configure advanced threat protection monitoring
    - Implement privileged access workstations for administrative access
    - Deploy change monitoring on all gateway servers
    - Configure tamper-evident logging

ANNEX B: Network Security Configuration

B.1 Kyndryl OPDG Network Security

1. **Network Segmentation**:

- Place OPDG servers in dedicated network segment
- Implement jump servers for administrative access
- Configure firewall rules allowing:
  - Outbound access to Azure Service Bus only
  - Inbound administrative access from approved management stations only
  - Internal access to required API endpoints only
- Block all other inbound/outbound traffic

2. **Enhanced Network Monitoring**:
   - Deploy network traffic analysis tools
   - Implement anomaly detection
   - Configure automated alerts for unusual traffic patterns
   - Establish baseline traffic patterns and monitor for deviations
   - Deploy network-based IDS/IPS solutions
3. **Network Traffic Protection**:
   - Implement TLS 1.3 with strong ciphers for all API communications
   - Configure Perfect Forward Secrecy for all encrypted sessions
   - Deploy mutual TLS authentication for all API endpoints
   - Implement certificate pinning where possible
   - Configure HSTS for all web communications

B.2 EDC OPDG Network Security

1. **DMZ Configuration**:
   - Configure DMZ segmentation according to defense-in-depth principles
   - Implement strict firewall rules for OPDG servers
   - Deploy network monitoring solutions
   - Configure logging of all network traffic
2. **Firewall Rules**:
   - Allow outbound access to Azure Service Bus only
   - Allow inbound administrative connections from approved sources only
   - Allow access to EDC API endpoints only
   - Block all other traffic

B.3 Security Monitoring and Incident Response

1. **Continuous Monitoring**:
   - Implement real-time monitoring of all OPDG traffic
   - Configure comprehensive logging with tamper-evident storage

- Deploy SIEM integration for centralized monitoring
- Configure automated alerts for security events

2. **Incident Response**:
   - Develop detailed response procedures for different incident types
   - Create runbooks for common security scenarios
   - Establish escalation paths with defined roles and responsibilities
   - Conduct regular tabletop exercises for different scenarios
   - Implement post-incident review procedures

ANNEX C: API Integration for Power Platform

C.1 API Security Documentation

1. **API Inventory and Classification**:
   - Document all API endpoints in both datacenters
   - Classify each API according to data sensitivity
   - Document authentication requirements for each API
   - Create API security testing plan
   - Establish API monitoring strategy
2. **Security Controls by Classification**:
   - Standard APIs (EDC):
     - TLS 1.2+ encryption
     - OAuth 2.0 authentication
     - Rate limiting
     - Input validation
   - Protected APIs (Kyndryl):
     - TLS 1.3 encryption with strong ciphers
     - Mutual TLS authentication
     - OAuth 2.0 with PKCE and short-lived tokens
     - Enhanced rate limiting
     - Advanced input validation and sanitization
     - IP restriction to OPDG servers only
     - Comprehensive audit logging

C.2 Power Platform Connection Configuration

1. **EDC Connections**:
   - In Power Platform Admin Center, navigate to Data Gateways

- Verify EDC gateway cluster is online and healthy
- Create connections to EDC data sources
- Configure authentication for each connection
- Apply clear naming convention (e.g., "EDC-ApiName")
- Test connections with minimal permissions

2. **Kyndryl Protected Connections**:
   - Verify Kyndryl gateway cluster is online and healthy
   - Create separate connections to Protected data sources
   - Apply clear naming convention (e.g., "PB-KYN-ApiName")
   - Configure enhanced authentication
   - Apply stricter data loss prevention policies
   - Implement connection usage monitoring
   - Configure alerts for unusual usage patterns

C.3 Connection Security Controls

1. **Standard Connection Security (EDC)**:
   - Implement connection encryption
   - Configure basic data loss prevention policies
   - Set up connection auditing
   - Implement connection monitoring
   - Establish connection recertification process
2. **Enhanced Connection Security (Kyndryl Protected)**:
   - Implement enhanced encryption settings
   - Configure strict data loss prevention policies
   - Implement comprehensive connection auditing
   - Deploy advanced connection monitoring
   - Configure alerts for usage anomalies
   - Establish quarterly connection recertification
   - Implement enhanced logging of all connection activities

ANNEX D: OPDG Governance Framework

D.1 Roles and Responsibilities

Role	Responsibilities	Department
OPDG Service Owner	Overall accountability for service	EC IT Operations

Role	Responsibilities	Department
EDC OPDG Administrators	Day-to-day management of EDC gateway	EC IT Support
Kyndryl OPDG Administrators	Day-to-day management of Kyndryl gateway	EC IT Security
Protected Security Officer	Security compliance for Protected data	EC IT Security
Change Approver	Review/approve changes	EC Change Advisory Board
API Owners	Management of specific APIs	Various EC Departments
Protected Data Custodian	Oversight of all Protected data handling	EC Data Governance
Security Monitoring Team	Continuous monitoring of gateway security	EC SOC Team
Incident Response Team	Response to security incidents	EC Security Operations

D.2 Enhanced Standard Operating Procedures

D.2.1 Gateway Maintenance

1. **EDC Gateway Maintenance**:
    - Schedule monthly maintenance window
    - Test updates in non-production environment
    - Create backup of configuration before updates
    - Apply updates during approved change window
    - Verify gateway functionality after updates
    - Document all maintenance activities
2. **Kyndryl Protected Gateway Maintenance**:
    - Schedule biweekly security patching
    - Conduct pre-deployment security assessment of updates
    - Create full system backup before any changes
    - Implement changes using four-eyes principle
    - Conduct post-update security verification

- Perform full functionality testing after updates
- Document all maintenance activities with detailed audit trail
- Conduct security review after each maintenance window

D.2.2 New Connection Onboarding

1. **Standard API Connection Process**:
   - Receive formal connection request with business justification
   - Conduct security assessment of requested API
   - Configure and test connection in development environment
   - Obtain security approval
   - Implement in production during change window
   - Document connection details in service catalog
2. **Protected API Connection Process**:
   - Receive formal connection request with detailed business justification
   - Conduct comprehensive security assessment of API
   - Verify API meets all Protected requirements
   - Perform threat modeling for the new connection
   - Conduct penetration testing of the API endpoint
   - Obtain security approval from Protected Security Officer
   - Implement in production during dedicated change window
   - Document detailed connection specifications in secure repository
   - Implement enhanced monitoring for new connection
   - Conduct post-implementation security review

D.2.3 Enhanced Monitoring and Incident Response

1. **Continuous Monitoring**:
   - Configure gateway performance monitoring for both environments
   - Implement real-time security monitoring for Protected gateway
   - Set up alerts for critical metrics with different thresholds by environment
   - Deploy behavioral analytics for Protected connections
   - Implement anomaly detection for all gateway traffic
   - Configure comprehensive audit logging
2. **Incident Response**:
   - Establish detailed incident response procedures by severity
   - Define clear escalation paths with 24/7 coverage for Protected
   - Create detailed incident response playbooks for different scenarios
   - Conduct quarterly incident response drills

- Implement post-incident review process
- Maintain dedicated incident response team for Protected data

ANNEX E: Enhanced Security for Protected

E.1 Protected Compliance Implementation

1. **Data Protection**:
   - Implement end-to-end encryption for all Protected data flows
   - Configure encryption at rest for all connection credentials
   - Deploy hardware security modules for key protection
   - Implement strict key rotation schedules
   - Configure data loss prevention policies
2. **Access Control**:
   - Implement multi-factor authentication for all administrative access
   - Deploy just-in-time privileged access management
   - Configure role-based access control with least privilege
   - Implement strict separation of duties
   - Conduct regular access reviews
   - Deploy privileged session monitoring
3. **Security Monitoring**:
   - Implement comprehensive audit logging
   - Configure tamper-evident log storage
   - Deploy continuous security monitoring
   - Implement behavioral analytics
   - Configure automated alerts for security anomalies
   - Conduct regular log reviews
   - Deploy honeypots and deception technology

E.2 ISO 27001 Controls Implementation for Protected

1. **Enhanced Information Security Policies**:
   - Develop Gateway-specific security policies
   - Implement detailed security procedures
   - Create comprehensive security standards
   - Establish regular policy review process
2. **Advanced Access Control**:
   - Implement privileged access workstations

- Deploy enhanced authentication mechanisms
- Configure strict session controls
- Implement automated access provisioning/deprovisioning
- Deploy access certification processes

3. **Cryptographic Controls**:
   - Implement cryptographic key management system
   - Deploy hardware security modules
   - Configure strong encryption algorithms
   - Implement certificate lifecycle management
   - Deploy advanced key protection measures
4. **Physical and Environmental Security**:
   - Implement strict physical access controls
   - Deploy environmental monitoring systems
   - Configure redundant power and cooling
   - Implement physical intrusion detection
   - Deploy CCTV monitoring
5. **Operations Security**:
   - Implement change management controls
   - Deploy capacity management processes
   - Configure backup and recovery procedures
   - Implement malware protection
   - Deploy technical vulnerability management
6. **Communications Security**:
   - Implement network segregation
   - Deploy secure network management
   - Configure information transfer policies
   - Implement secure messaging
   - Deploy network security monitoring

E.3 Enhanced Security Monitoring and Assessment

1. **Continuous Security Monitoring**:
   - Implement real-time monitoring of gateway health
   - Deploy behavior-based anomaly detection
   - Configure automated alerting for security events
   - Implement correlation of security logs
   - Deploy user behavior analytics
2. **Regular Security Assessments**:

- Schedule monthly vulnerability assessments
- Conduct quarterly penetration testing
- Perform bi-annual security architecture review
- Implement continuous compliance monitoring
- Deploy configuration baseline monitoring
- Conduct regular threat modeling exercises

3. **Security Reporting**:
   - Generate weekly security metrics reports
   - Conduct monthly security posture reviews
   - Implement quarterly compliance assessments
   - Deploy executive security dashboards
   - Generate comprehensive annual security reports

Implementation Action Plan

- [ ] Document current network topology between EDC and Kyndryl
- [ ] Identify and catalog all API endpoints in both datacenters with data classification
- [ ] Provision servers for OPDG in Kyndryl datacenter
- [ ] Implement enhanced security hardening for Kyndryl servers
- [ ] Install and configure OPDG cluster in EDC following Annex A procedures
- [ ] Install and configure OPDG cluster in Kyndryl following enhanced security procedures
- [ ] Register both gateways with Elections Canada Power Platform tenant
- [ ] Implement comprehensive security monitoring for both gateway clusters
- [ ] Create secure connections to APIs in Power Platform for each gateway
- [ ] Validate connectivity with test transactions for each environment
- [ ] Implement monitoring and alerting according to Annex D
- [ ] Document final configuration in Elections Canada CMDB
- [ ] Conduct security assessment of complete implementation
- [ ] Obtain authorization to operate from EC security team for each gateway

Conclusion

The implementation of dedicated OPDG clusters in both datacenters (Option 1) establishes the most secure approach for enabling Power Platform access to APIs in Elections Canada's environments, particularly for Protected data in the Kyndryl datacenter. This design eliminates cross-datacenter traffic for Protected data and creates clear security boundaries between different data classification levels.

By implementing separate gateways:

1. Protected data remains within its security boundary until securely transmitted to Power Platform
2. Each gateway is optimized for its specific security requirements
3. Security monitoring is simplified with clear separation of environments
4. Compliance with Government of Canada security standards is enhanced

While other options remain viable based on specific requirements, the dedicated OPDG approach provides the strongest security posture for Protected data and clearest alignment with security best practices.

For technical implementation support, engage with Microsoft Premier Support or Elections Canada's approved Microsoft partner with expertise in Power Platform and secure networking implementations, particularly those with experience in Protected environments.

References and Resources

Microsoft Documentation

- On-Premises Data Gateway Official Documentation
- Install On-Premises Data Gateway in Cluster Mode
- Power Platform Admin Center - Data Gateway Management
- On-Premises Data Gateway Architecture
- Troubleshooting the On-Premises Data Gateway
- Power Automate - Manage Connections

Government of Canada Security Standards

- ITSG-22: Baseline Security Requirements for Network Security Zones
- ITSG-33: IT Security Risk Management
- Government of Canada Cloud Security Risk Management Approach and Procedures
- Protected Information Management Guidelines

ISO Standards

- ISO/IEC 27001:2022 Information Security Management
- ISO/IEC 27017:2015 Cloud Security
- ISO/IEC 27018:2019 Protection of PII in Public Clouds

Technical Resources

- Microsoft Power Platform Center of Excellence (CoE) Starter Kit
- Gateway Performance Monitoring
- TLS 1.2 Implementation Guide
- Power Platform API Security Best Practices
- Networking with ExpressRoute for Power Platform

Elections Canada Specific Resources

- Elections Canada IT Security Policy (internal document reference tbd)
- Elections Canada Cloud Security Standards (internal document reference tbd)
- Elections Canada Enterprise Architecture Guidelines (internal document reference tbd)
- Elections Canada Data Classification Standards (internal document reference tbd)
- On-Premises Data Gateway Configuration for Elections Canada Multi-Datacenter API Access (tbd-current doc with chosen architecture/implementation)