API Management v Praxi
Konference Kybernetická Bezpečnost
Praha, 20. 09. 2017

Zdeněk Borůvka
European Technical Team Leader
IBM Hybrid Cloud | Hybrid Integration
Messaging, Integration, API Economy & Mobile
API (Driven) World

Today API means more than just “Application Programming Interface”. It’s a new way to interact with your clients and partners which allows to create innovative business models on top of existing enterprise assets and services.
The PSD2 expands the reach of the original PSD, including also what is referred to as “one leg out” transactions where at least one party is located within EU borders.

PSD2 influences financial transactions outside of the EU:

October 2015  
PSD2 becomes official

December 2015  
PSD2 enters Official Journal of EU

June 2016  
Security standards

January 2017  
Technical standards

Late 2018  
PSD2 Live

PSD2 and the Open Banking Pattern

Banks

Third-party Providers (TPPs)
Account Information Service Providers (AISPs)
Payment Initiation Service Providers (PISPs)

Account Information Service (AIS)

Payment Initiation Service (PIS)

Consumers
Telco
Telemanagement Forum announced its Open API recommendations in 2016. All major Telco operators instantly accepted it.

Public
APIs for Government data:
- UK
- USA
- India
- Russia
- etc

Healthcare
FHIR Framework
More than 1500 participants from 50 countries

Twitter
Generates more than 13 billion API calls per day

Netflix
Serves more than 1.5 billion API calls per day

Google
Handles more than 9 billion API calls per day
What is Needed to Build Good APIs?

- Implementation
- API strategy
- Monetization models
- Application development
- Security
- API Development
API Foundation: IBM API Connect

- Developer Portal
- API Management Node
- Collective Controller
- Microservices App Computer Runtime (Node.js/Java)
- API Gateway (DataPower/MicroGW)
- Developer Toolkit
- Database
- Cloud
- App Server
- ESB Middleware
- System I

External developers
Partner developers
Internal developers
Mobile Apps
Partner services
Enterprise services
IoT

API Traffic
The Security Aspect...

- TLS profiles
  - Self-signed certificates
  - PKCS#12 files for CA
- TLS communication between the Management node and the API Gateway
- Database encryption
- User registries: Local (Default), LDAP, Authentication URL
- Accounts and Passwords expirations
- Gateway level security
### IBM DataPower Gateway (Base)

#### Secure
- Authentication, authorization
- Security token translation
- Service / API virtualization
- Threat protection
- Message schema validation
- Message filtering
- Message digital signature
- Message encryption
- AV scanning integration

#### Integrate
- Transport protocol bridging
- Any-to-any message transformation
- Message enrichment
- Database connectivity
- Mainframe connectivity
- B2B partner connectivity
- Hybrid cloud connectivity

#### Control & Manage
- Quota & rate enforcement
- Content-based routing
- Message accounting
- B2B partner management
- Integration w/ governance, management & monitoring platforms including IBM API Connect & WSRR for policy enforcement

#### Optimize & Offload
- HTTP/2
- SSL / TLS offload
- Hardware accelerated crypto*
- JSON, XML offload
- JavaScript, JSONiq, XSLT, XQuery acceleration
- Local response caching
- Distributed caching with WXS
- Backend load balancing

---

### ISAM Proxy Module
- User access control, session management, web SSO enforcement
- Advanced mobile security: mobile SSO, context-based access, one-time password, multi-factor authn

### Application Optimization Module
- Frontend self-balancing
- Backend intelligent load distribution
- Session affinity
- z Sysplex Distributor integration

### TIBCO EMS Module
- Integrate with TIBCO EMS messaging middleware
- Support for queues & topics
- Load balancing & fault-tolerance

### Integration Module
- Any-to-Any message transformation
- Database connectivity
- Mainframe IMS connectivity

---

Single, modular & extensible Gateway platform not only for APIs
Supported standards and protocols

- **Data format & language**
  - JavaScript
  - JSON
  - JSON Schema
  - REST, SOAP 1.1, 1.2
  - WSDL 1.1
  - XML 1.0
  - XML Schema 1.0
  - XPath 1.0, XPath 2.0 (XQuery only)
  - XSLT 1.0
  - XQuery 1.0, JSONiq

- **Security policy enforcement**
  - OAuth 2.0, OpenID Connect, Social Login
  - JWE, JWS, JWT, JWK
  - SAML 1.0/1.1/2.0, SAML Tkn Profile, SAML queries
  - XACML 2.0
  - Kerberos (including S4U2Self, S4U2Proxy)
  - SPNEGO
  - RADIUS, RSA SecurID OTP using RADIUS
  - LDAP versions 2 and 3
  - Lightweight Third-Party Authentication
  - Microsoft Active Directory
  - FIPS 140-2 Level 3 (w/ optional HSM)
  - FIPS 140-2 Level 1 (w/ certified crypto module)
  - SAF & IBM RACF® integration with z/OS
  - Internet Content Adaptation Protocol
  - W3C XML Encryption
  - W3C XML Signature
  - S/MIME encryption and digital signature
  - WS-Security 1.0, 1.1
  - WS-I Basic Security Profile 1.0, 1.1
  - WS-SecurityPolicy
  - WS-SecureConversation 1.3

- **Transport & connectivity**
  - HTTP, HTTP/2, HTTPS, WebSocket Proxy
  - FTP, FTPS, SFTP
  - WebSphere MQ
  - WebSphere MQ File Transfer Edition
  - TIBCO EMS
  - WebSphere Java Message Service
  - IBM IMS Connect, & IMS Callout
  - NFS
  - AS1, AS2, AS3, AS4, ebMS 2.0, CPPA 2.0, POP, SMTP (B2B Module)
  - DB2, Microsoft SQL Server, Oracle, Sybase, IMS

- **Transport Layer Security**
  - TLS versions 1.0, 1.1, and 1.2
  - SSL versions 2 and 3
  - SNI, PFS, ECC Ciphers

- **Public key infrastructure (PKI)**
  - RSA, 3DES, DES, AES, SHA, X.509, CRLs, OCSP
  - PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12
  - XKMS for integration with Tivoli Security Policy Manager (TSPM)

- **Management**
  - Simple Network Management Protocol
  - SYSLOG
  - IPv4, IPv6

- **Web services**
  - WS-I Basic Profile 1.0, 1.1
  - WS-I Simple SOAP Basic Profile
  - WS-Policy Framework
  - WS-Policy 1.2, 1.5
  - WS-Trust 1.3
  - WS-Addressing
  - WS-Enumeration
  - WS-Eventing
  - WS-Notification
  - Web Services Distributed Management
  - WS-Management
  - WS-I Attachments Profile
  - SOAP Attachment Feature 1.2
  - SOAP with Attachments (SwA)
  - Direct Internet Message Encapsulation
  - Multipurpose Internet Mail Extensions
  - XML-binary Optimized Packaging (XOP)
  - Message Transmission Optimization Mechanism (MTOM)
  - WS-MediationPolicy (IBM standard)
  - Universal Description, Discovery, and Integration (UDDI versions 2 and 3), UDDI version 3 subscription
  - WebSphere Service Registry and Repository (WSRR)
Why IBM API Connect

**LOWER PROJECT RISK**
- Local Experienced SMEs
- European Team Working on API Projects
- Proven Ability to Quickly Involve Labs if Needed

**IBM AS A PARTNER**
- Listening to Your Feedback on Our Product (Labs)
- Quick Escalation Contact to the Labs

**CLOUD READY**
- Start onPrem and Move to the Cloud if Interested
- Run Your Solution in Hybrid Mode (onPrem/Cloud)
- Use our Cloud or Other Cloud Vendors if Needed

**HUGE EXPERIENCE FROM PSD2 (and other) PROJECTS**
- Key Banks in Europe Building their PSD2 Solution on IBM APIC
- Our Team Helping Them with Innovation and Technical Solution
- Close Collaboration with Partners is Well Proven Model

© 2017 IBM Corporation
Where can I learn more about IBM DataPower Gateway?

- **DP Overview Video:** [youtube.com/watch?v=RqT3f_TmSMM](youtube.com/watch?v=RqT3f_TmSMM)
- **DP Developer Center & Playground:** [developer.ibm.com/datapower/](developer.ibm.com/datapower/)
- **DP Product Documentation:** [ibm.com/support/knowledgecenter/SS9H2Y](ibm.com/support/knowledgecenter/SS9H2Y)
- **DP Videos:** [youtube.com/channel/UCV2__gdea5LM58S-E3WCqew](youtube.com/channel/UCV2__gdea5LM58S-E3WCqew)
- **DP Slide Decks:** [http://slideshare.net/ibmdatapower](http://slideshare.net/ibmdatapower)
- **API Connect Knowledge Center:**
  [https://www.ibm.com/support/knowledgecenter/en/SSMNED_5.0.0/mapfiles/getting_started.html](https://www.ibm.com/support/knowledgecenter/en/SSMNED_5.0.0/mapfiles/getting_started.html)
- **API Connect Developer portal:**
- **Bluemix Public:** [https://console.ng.bluemix.net](https://console.ng.bluemix.net)
- **Open banking Sandbox:** [https://live-open-banking.developer.eu.apiconnect.ibmcloud.com](https://live-open-banking.developer.eu.apiconnect.ibmcloud.com)
API Management v Praxi
Konference Kybernetická Bezpečnost
Praha, 20. 09. 2017

Zdeněk Borůvka
European Technical Team Leader
IBM Hybrid Cloud | Hybrid Integration
Messaging, Integration, API Economy & Mobile
Available Form Factors: Deploy Anywhere

**Physical**
- Gateway Image
  - Signed & Encrypted Gateway Stack
  - IBM Optimized Embedded OS
- Hardware
  - Trusted Platform Module
  - Hardware Security Module
- Crypto Acceleration

**Virtual**
- Gateway Image
  - Signed & Encrypted Gateway Stack
  - IBM Optimized Embedded OS
- Hypervisor
  - Hardware
- Crypto Acceleration

**Linux**
- Gateway Image
  - Signed & Encrypted Gateway Stack
  - IBM Optimized Application Layer
- Operating System
  - Hardware / Hypervisor
  - IBM Optimized Application Layer

**Docker**
- Gateway Image
  - IBM Optimized Application Layer
- Operating System
  - Hardware / Hypervisor

All in one solution (HW / SW)
- * Physical security
- * Drop-in deployment & mgmt
- * Performance including HW crypto acceleration
- * DMZ drop-in
- Embedded HSM option (FIPS 140-2 certified)

Software solution (Virtual machine)
- * User responsible for providing & securing HW and Hypervisor
- Flexible deployment
- Flexible resource allocations

Software solution (Application)
- * User responsible for providing & securing HW, Hypervisor, OS
- Public & private Cloud deployments
- Rapid scale up/down
- First class Cloud citizen
- Physical server deployment

Software solution (Container)
- * User responsible for providing & securing HW, Hypervisor, OS
- Docker optimized image
- * Apply your DevOps tools & processes
- * Use Docker Volumes & Docker Build to manage gateway config

1 Supported on VMware & Citrix XenServer hypervisors.
2 Supported via RHEL & Ubuntu operating systems anywhere, including bare-metal physical servers, hypervisors (Hyper-V, KVM, VMware, XenServer) and cloud platforms (Amazon EC2, Microsoft Azure, IBM SoftLayer, Cloud Foundry, OpenShift, others).

**“Once deployed, it’s DataPower Gateway”**

**“Available in Production, Non-prod & Developer edition on X86_64”**

Available free of charge for Development use:
[https://hub.docker.com/r/ibmcom/datapower/](https://hub.docker.com/r/ibmcom/datapower/)