API Management v Praxi

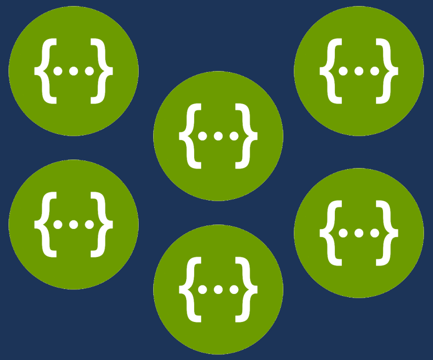
Konference Kybernetická Bezpečnost
Praha, 20. 09. 2017

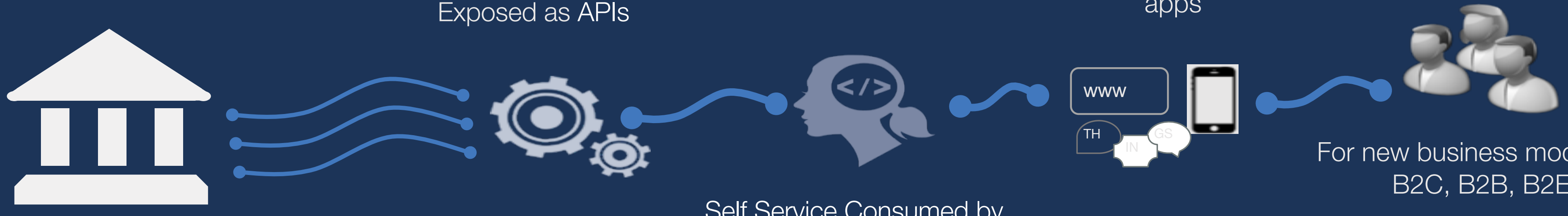
Zdeněk Borůvka

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.





Exposed as APIs

To develop innovative apps

Business Assets

Self Service Consumed by Developers

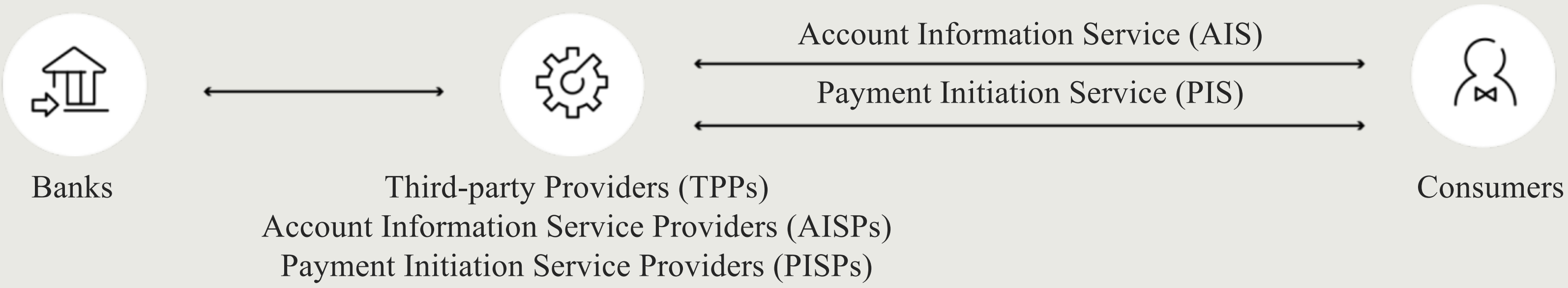
For new business models for B2C, B2B, B2E

PSD2 and the Open Banking Pattern

PSD2 influences financial transactions outside of the EU:

> *“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.”*

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



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

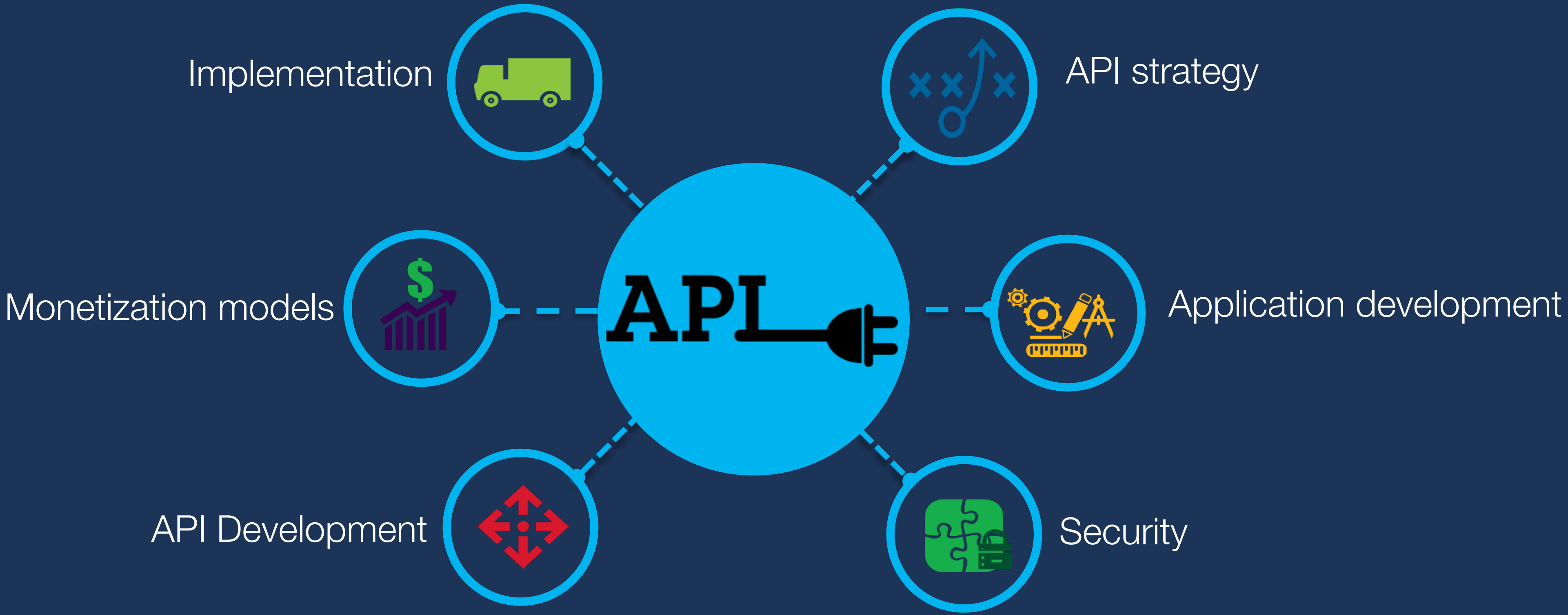
FHIR Framework
More than 1500 participants from 50 countries

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

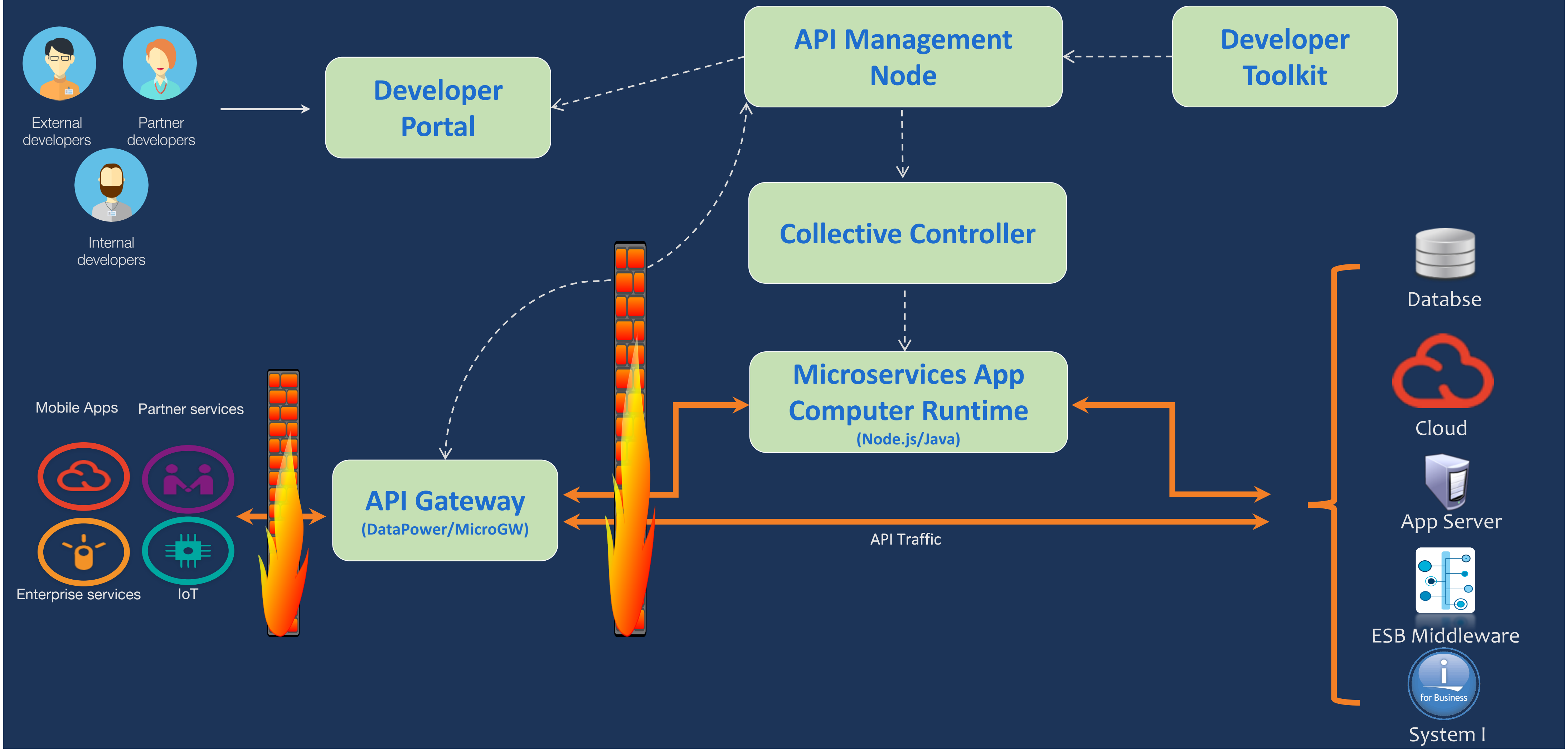
Monetization models

Application development

API Development

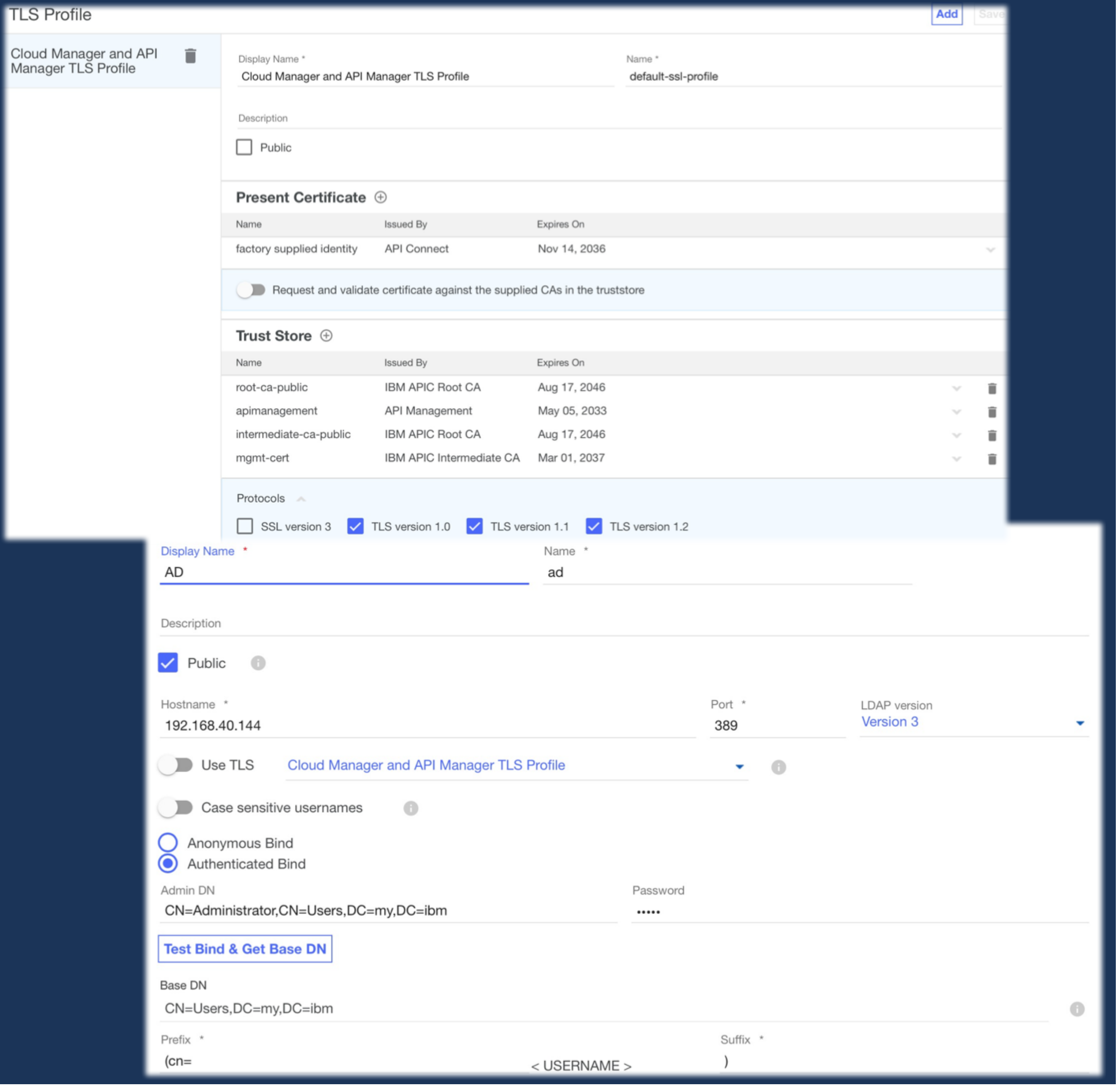
Security

API Foundation: **IBM API Connect**



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



Display Name *: Cloud Manager and API Manager TLS Profile

Name *: default-ssl-profile

Description

□ Public

Present Certificate ⊕

Name	Issued By	Expires On
factory supplied identity	API Connect	Nov 14, 2036

Request and validate certificate against the supplied CAs in the truststore

Trust Store ⊕

Name	Issued By	Expires On
root-ca-public	IBM APIC Root CA	Aug 17, 2046
apimanagement	API Management	May 05, 2033
intermediate-ca-public	IBM APIC Root CA	Aug 17, 2046
mgmt-cert	IBM APIC Intermediate CA	Mar 01, 2037

Protocols

□ SSL version 3 ☑ TLS version 1.0 ☑ TLS version 1.1 ☑ TLS version 1.2

Display Name *: AD

Name *: ad

Description

☑ Public

Hostname *: 192.168.40.144

Port *: 389

LDAP version: Version 3

Use TLS: Cloud Manager and API Manager TLS Profile

Case sensitive usernames

○ Anonymous Bind
● Authenticated Bind

Admin DN: CN=Administrator,CN=Users,DC=my,DC=ibm

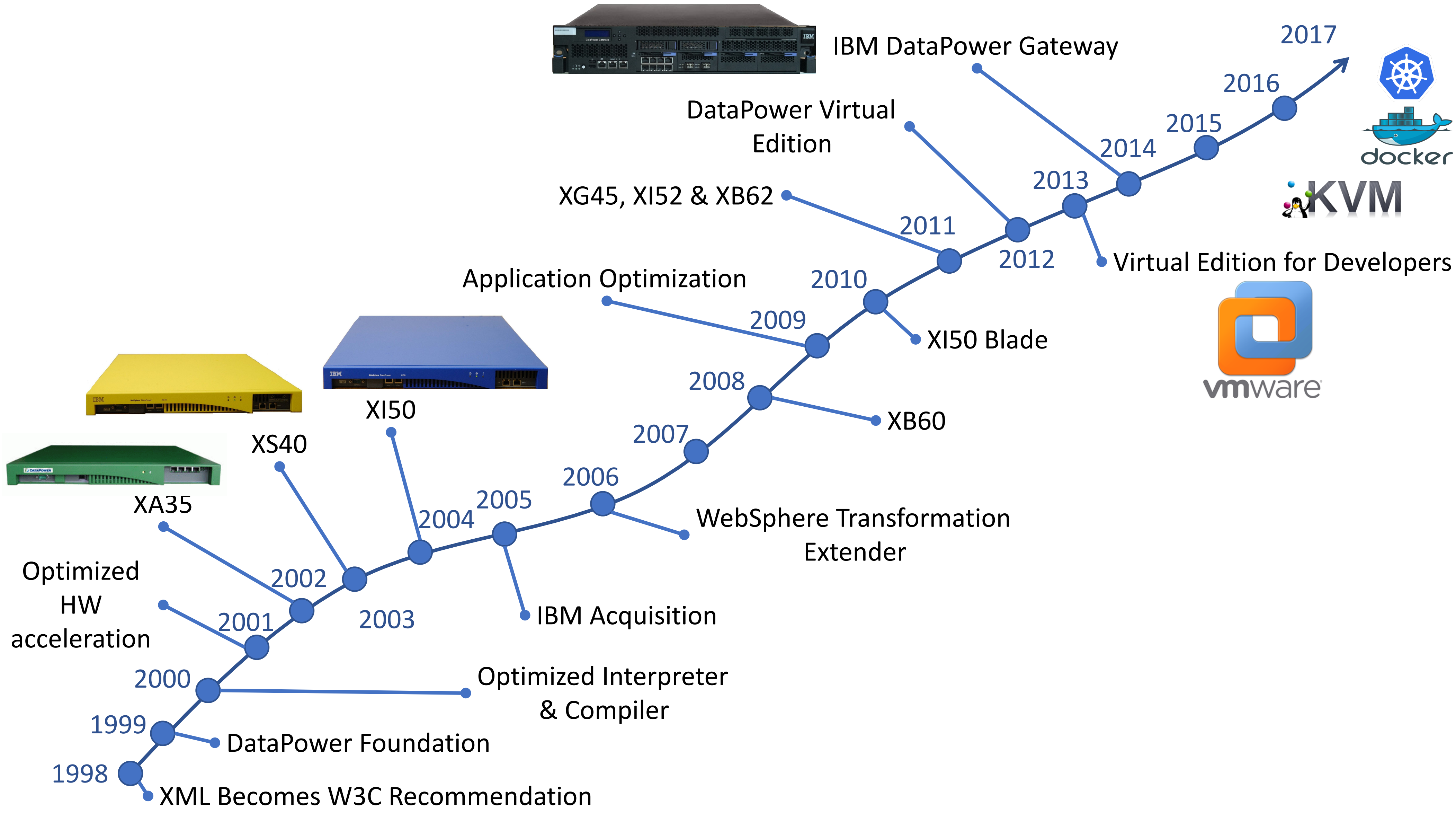
Password: •••••

Base DN: CN=Users,DC=my,DC=ibm

Prefix *: (cn=

< USERNAME >

Suffix *:)



1998 XML Becomes W3C Recommendation

1999 DataPower Foundation

2000 Optimized Interpreter & Compiler

2001 Optimized HW acceleration

2002 XA35

2002 XS40

2003

2004 XI50

2005 IBM Acquisition

2006 WebSphere Transformation Extender

2007

2008 XB60

2009 Application Optimization

2010 XI50 Blade

2011 XG45, XI52 & XB62

2012 DataPower Virtual Edition

2013 Virtual Edition for Developers

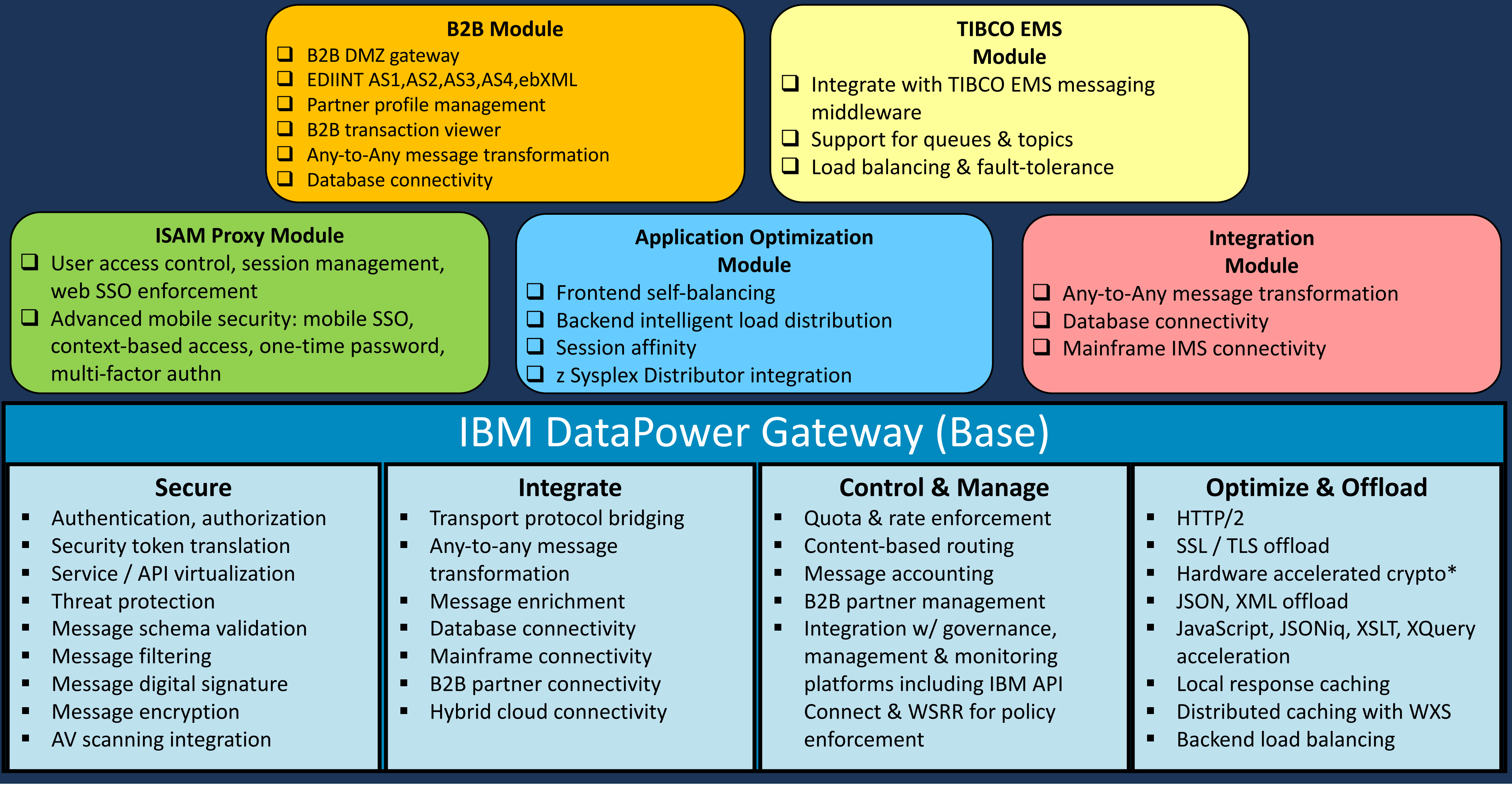
2014 IBM DataPower Gateway

2015

2016

2017

Single, modular & extensible Gateway platform not only for APIs



B2B Module

- □ B2B DMZ gateway
- □ EDIINT AS1,AS2,AS3,AS4,ebXML
- □ Partner profile management
- □ B2B transaction viewer
- □ Any-to-Any message transformation
- □ Database connectivity

TIBCO EMS Module

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

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

Integration Module

- □ Any-to-Any message transformation
- □ Database connectivity
- □ Mainframe IMS connectivity

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

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

Where can I learn more about IBM DataPower Gateway?

- DP Overview Video: youtube.com/watch?v=RqT3f_TmSMM
- DP Product Page: ibm.com/software/products/en/datapower-gateway
- DP Developer Center & Playground: developer.ibm.com/datapower/
- DP Product Documentation: ibm.com/support/knowledgecenter/SS9H2Y
- DP Videos: youtube.com/channel/UCV2_-gdea5LM58S-E3WCqew
- DP Slide Decks: http://slideshare.net/ibmdatapower
- DP playground: https://developer.ibm.com/datapower/docker/
- API Connect Knowledge Center: https://www.ibm.com/support/knowledgecenter/en/SSMNED_5.0.0/mapfiles/getting_started.html
- API Connect Developer portal: https://www.ibm.com/support/knowledgecenter/en/SSMNED_5.0.0/com.ibm.apic.devportal.doc/tutorials_devportal_home.html
- Bluemix Public: https://console.ng.bluemix.net
- Open banking Sandbox: https://live-open-banking.developer.eu.apiconnect.ibmcloud.com

API Management v Praxi

Konference Kybernetická Bezpečnost
Praha, 20. 09. 2017

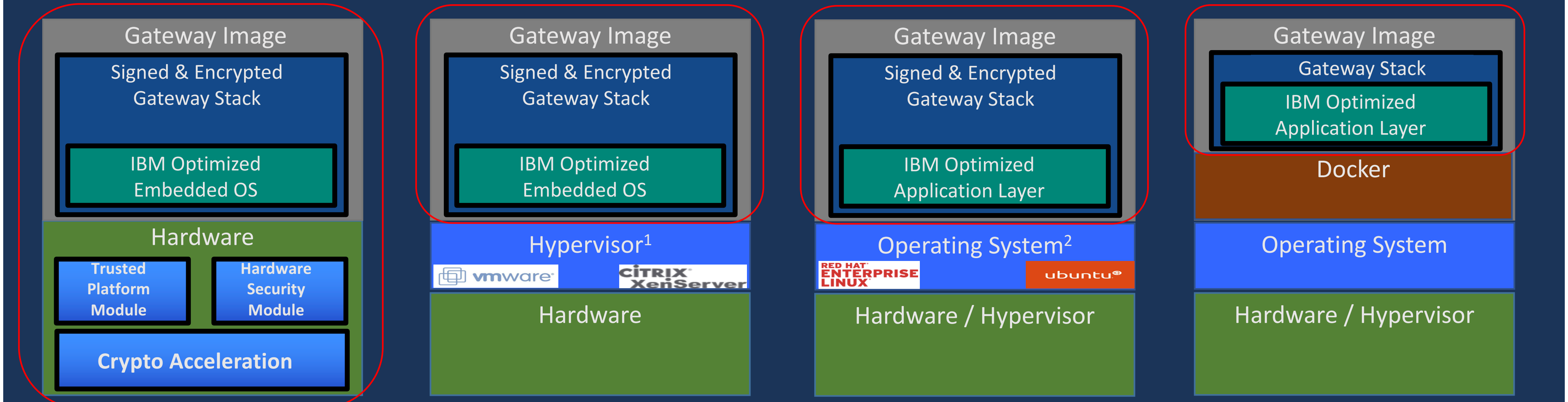
Zdeněk Borůvka

European Technical Team Leader
IBM Hybrid Cloud | Hybrid Integration
Messaging, Integration, API Economy & Mobile

SIT
Simplified IT

Available Form Factors: Deploy Anywhere

IBM Provided ▭



Physical

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

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)

Virtual**

- Gateway Image
  - Signed & Encrypted Gateway Stack
    - IBM Optimized Embedded OS
- Hypervisor[1]
  - vmware
  - CITRIX XenServer
- Hardware

Software solution (**Virtual machine**)
  * User responsible for providing & securing HW and Hypervisor

Flexible deployment

Flexible resource allocations

Linux**

- Gateway Image
  - Signed & Encrypted Gateway Stack
    - IBM Optimized Application Layer
- Operating System[2]
  - RED HAT ENTERPRISE LINUX
  - ubuntu
- Hardware / Hypervisor

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

Docker**

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

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/*