Building Mobile Ready Back-ends & Secure APIs

Data Center Apps

Service/API Gateway
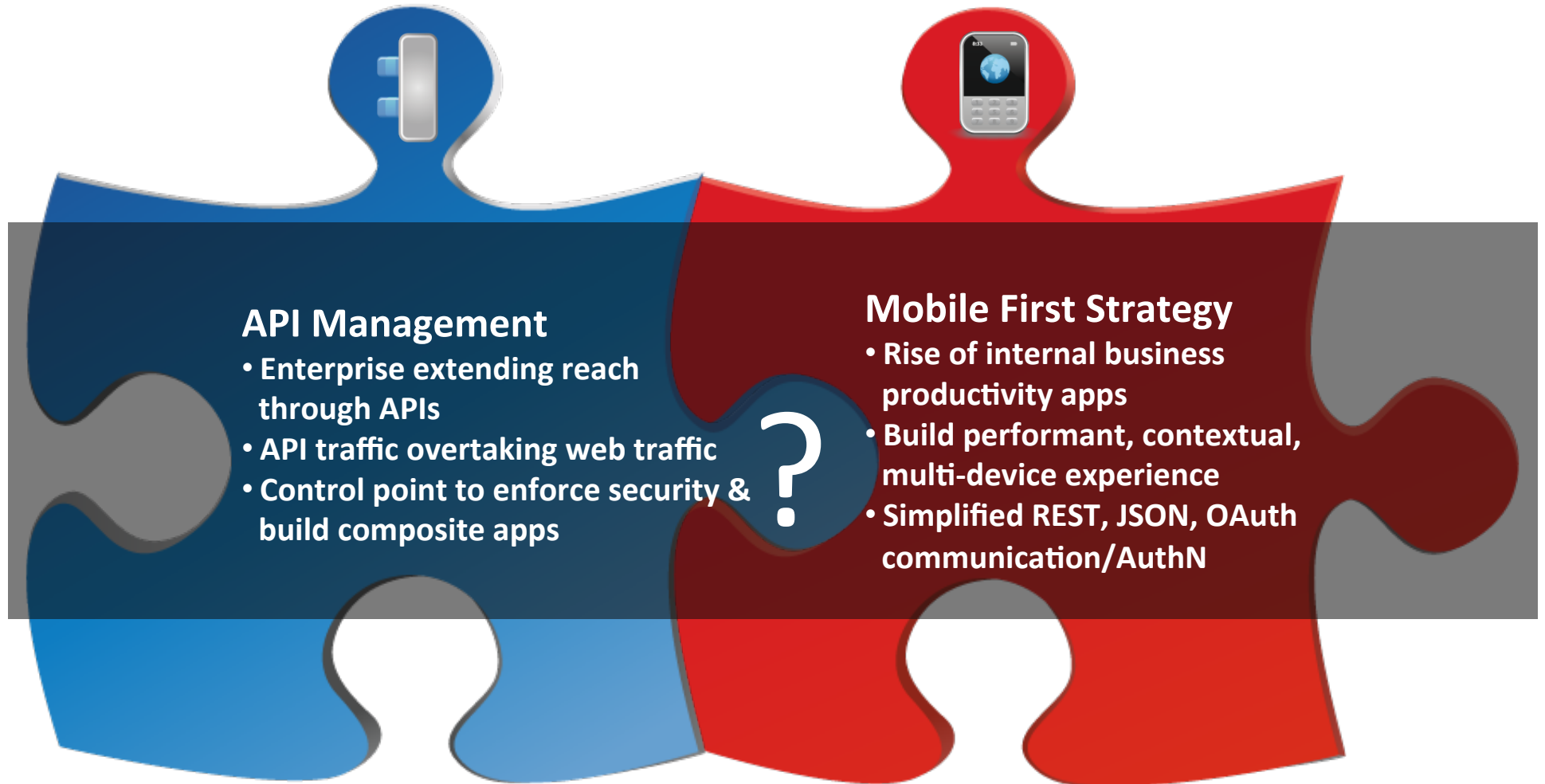
API
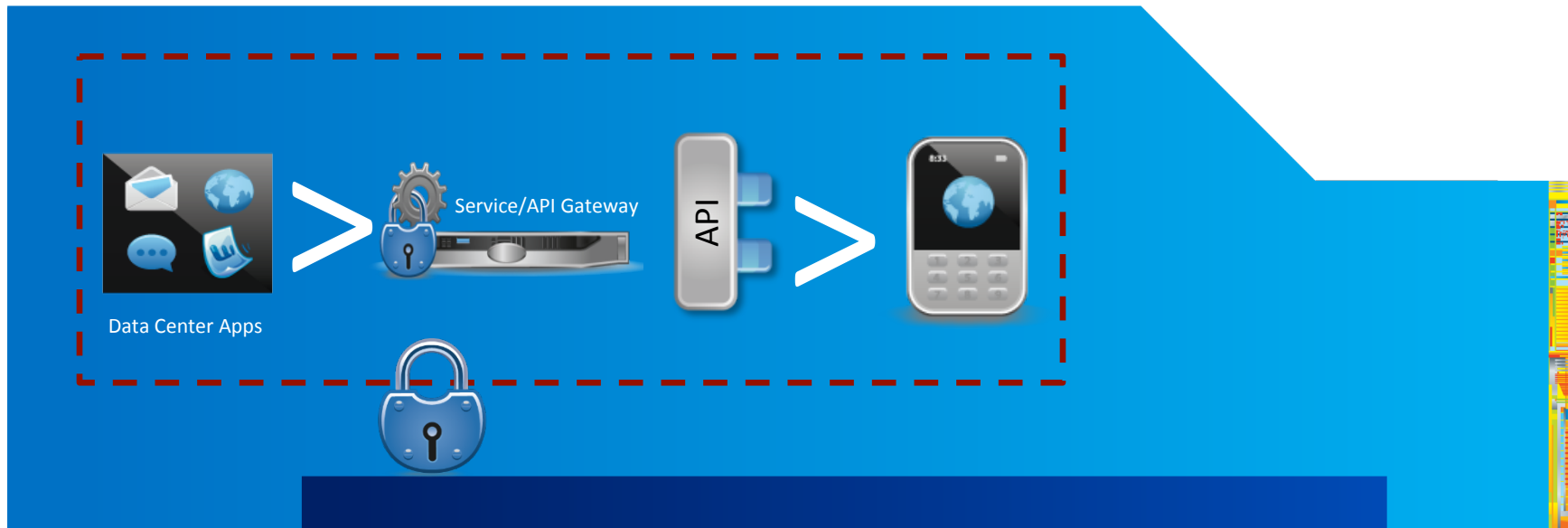
Blake Dournaee, Product Manager, Intel
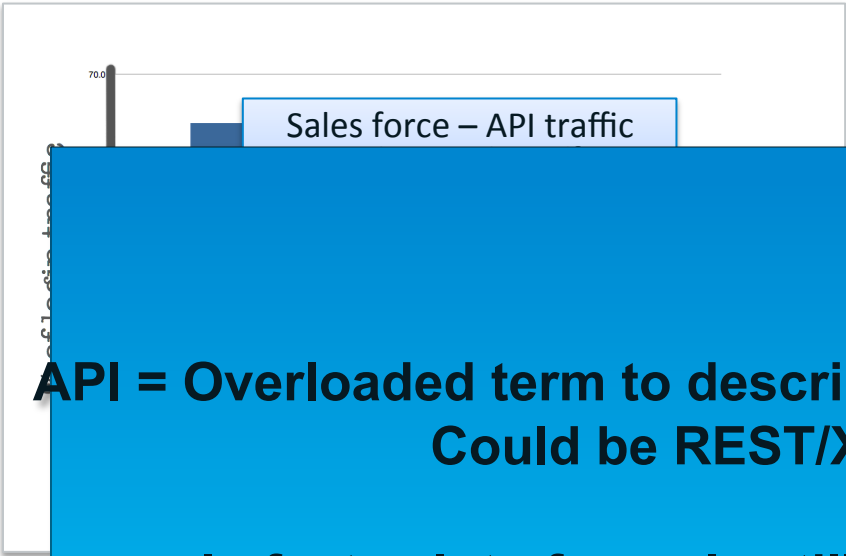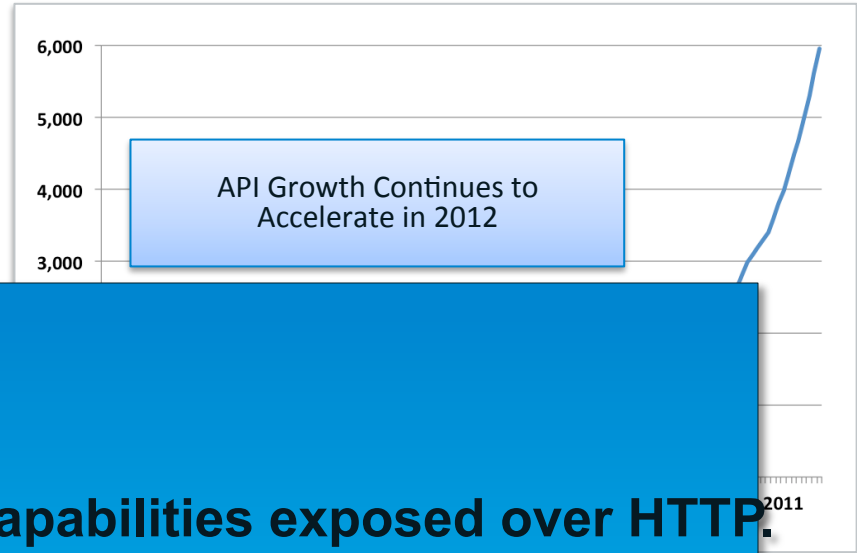Data Center Software Division

Agenda

- Trends: APIs and Mobile

- Challenges of exposing services to clients

- First mile, middle tier, last mile integration

- Gateway Paradigm

- Unified Mobile Architecture

- Intel Product

Two Red Hot Trends - How do they Intersect?

API Management
- Enterprise extending reach through APIs
- API traffic overtaking web traffic
- Control point to enforce security & build composite apps

?

Mobile First Strategy
- Rise of internal business productivity apps
- Build performant, contextual, multi-device experience
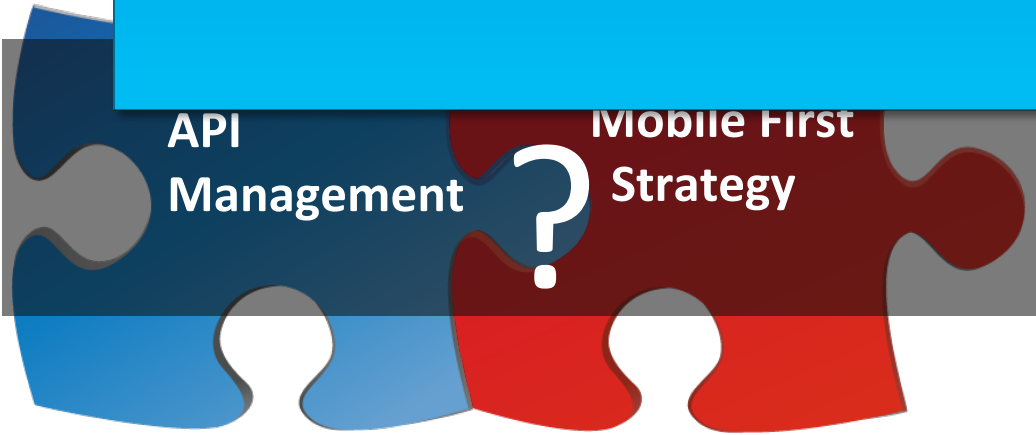- Simplified REST, JSON, OAuth communication/AuthN

60% of all logins to the popular Salesforce.com platform are through RESTful APIs, and 40% are through traditional browsers.

(intel)

API Shift – It's Here

Sales force – API traffic

API Growth Continues to
Accelerate in 2012

6,000

5,000

4,000

3,000

70.0

2011

**API = Overloaded term to describe capabilities exposed over HTTP.
Could be REST/XML/JSON or SOAP**

In fact, a lot of people still use SOAP in the Enterprise

**API
Management**

?

**Mobile First
Strategy**

NETFLIX   1.4 billion API calls / **day** (May 2012)

KLOUT   1 billion API calls / **day** (May 2012)

Expedia
Affiliate Network $2 billion via APIs / **Year** (May 2012)

MASHERY   Billions of API calls / **month** (May 2012)

(intel)

Primary API Management Enablement Challenges

Orchestration

REST Façade "Proxy"

Secure APIs

Mobile & App Firewalling

AAA

Lightweight Mobile AuthN

API Sharing & Monetization

API Sharing Portal

Fast Changing Mobile APIs

Multi-Channel Versioning

Cloud Service Brokering

IT as a Broker

(intel)

Architectural Challenges
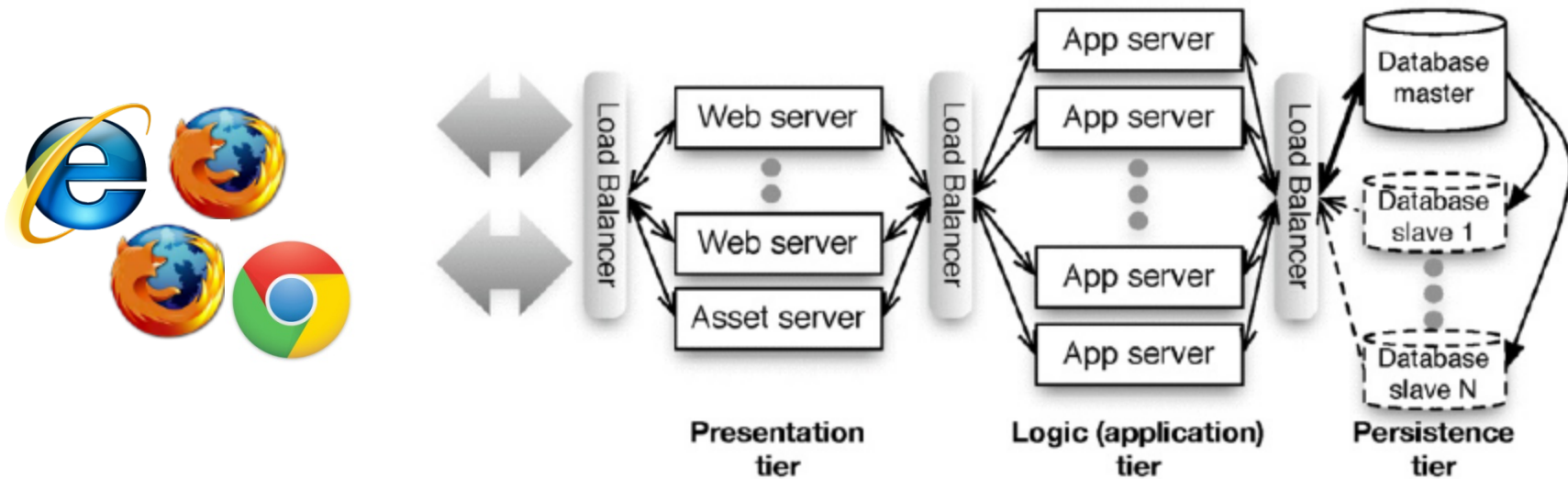
3-Tier Shared Nothing Architecture
- Most common architecture, widely deployed
- Gold standard, developed as a result of the web revolution
- **Problem:** Designed primarily for HTML web browsers, *not mobile apps*

Image borrowed from *Software engineering for Software as a Service; Coursera course by Armando Fox, Dave Patterson*

(intel)

Native vs. Web Mobile Apps

	Native	Web
App Type	Runs on phone operating system directly). Faster UI performance. Controls download at installation	Runs in browser or O/S container. Slower UI downloaded on-demand; code written in abstraction layer of web technologies (Javascript, CSS, HTML5).
Security Posture	Phone access to file system for read/write. Security beyond https requires custom code. Susceptible to malware	Basic security confined to https. Protocols such as OAuth require toolkit. Browser wrapper provides sandbox
Server Arch	Mix of custom middleware & software often needs own ESB	Similar to web server/app server model with content optimization

So… what's the answer? Who wins?

Answer #1:

Both

Answer #2:

Native will always have the edge due to handset differentiation, despite advancing standards

(intel)

Enterprises Have Unique Requirements for Mobile Enablement

Are trying to get a mobile project going at your Enterprise?

Does this look familiar?

Disparate middleware and database technologies

Disparate identity management silos

Disparate programming languages

Current architecture optimized for **web browsers**

Vertical integration prohibits cloud outsourcing

Inconsistent security model across domains

WARNING
CHALLENGES AHEAD

On top of this you want:

(intel)

Building the App - Architecture

Application Requirements

- Retail Sales Manager – Uses Tablet, no Laptop

- Needs to query store revenue information
  - Store name, city, state, revenue

- Needs to post new hire PII information
  - Name, address, phone number, SSN, drivers license #

?

Enterprise Boundary

RESTful Service — Ruby On Rails ◇ RDBMS

CRUDable Interface

SOAP — SAP Business Suite

Query as a Web Service

Active Directory

Enterprise Identities

(intel)

Gateway Design Pattern

When

- Architectural best practice for API or web services communication
- Product agnostic
- Relies on indirection to solve security, performance and management problems
- Ideal for application to application traffic

```
                HTTP                    HTTP
 ┌─────────┐  ────────▶  ┌─────────┐  ────────▶  ┌──────────────┐
 │         │             │         │             │              │
 │ Client  │             │ Gateway │             │ Application  │
 │         │             │         │             │   Server     │
 │         │  ◀────────  │         │  ◀────────  │              │
 └─────────┘  HTTP/XML   └─────────┘  HTTP/XML   └──────────────┘
              HTTP/JSON
```

All problems in computer science can be solved by another level of indirection- David Wheeler

"...except for the problem of too many layers of indirection." – Kevlin Henny

(intel)
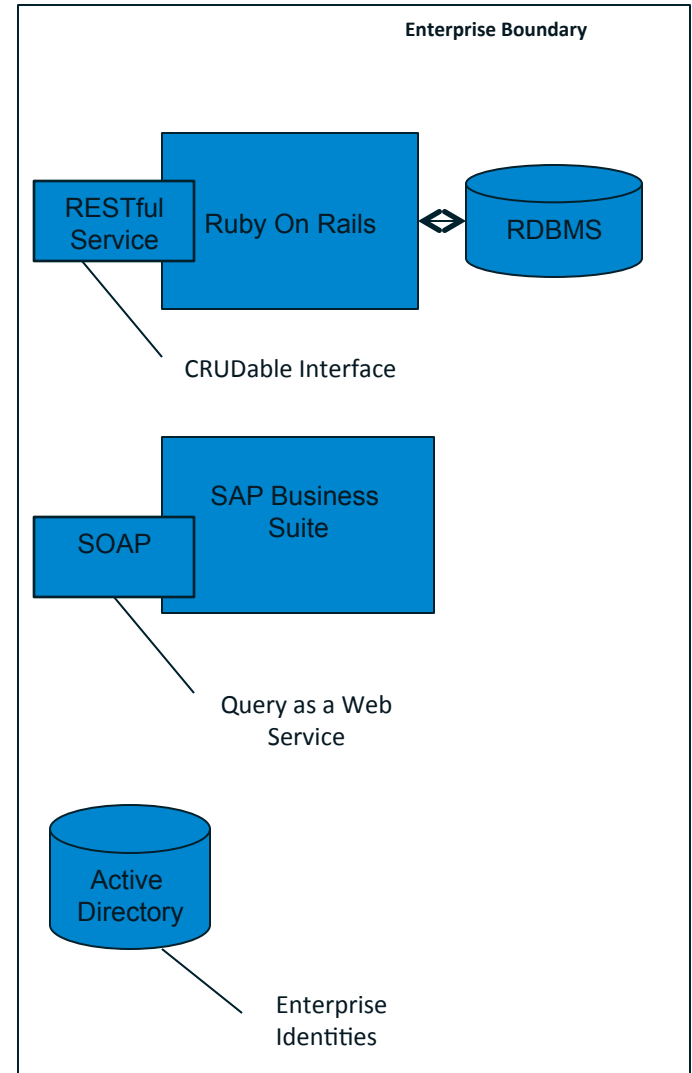
Gateway Design Pattern

When

- Architectural best practice for API or web services communication
- Product agnostic
- Relies on indirection to solve security, performance and management problems
- Ideal for application to application traffic

All problems in computer science can be solved by another level of indirection- David Wheeler

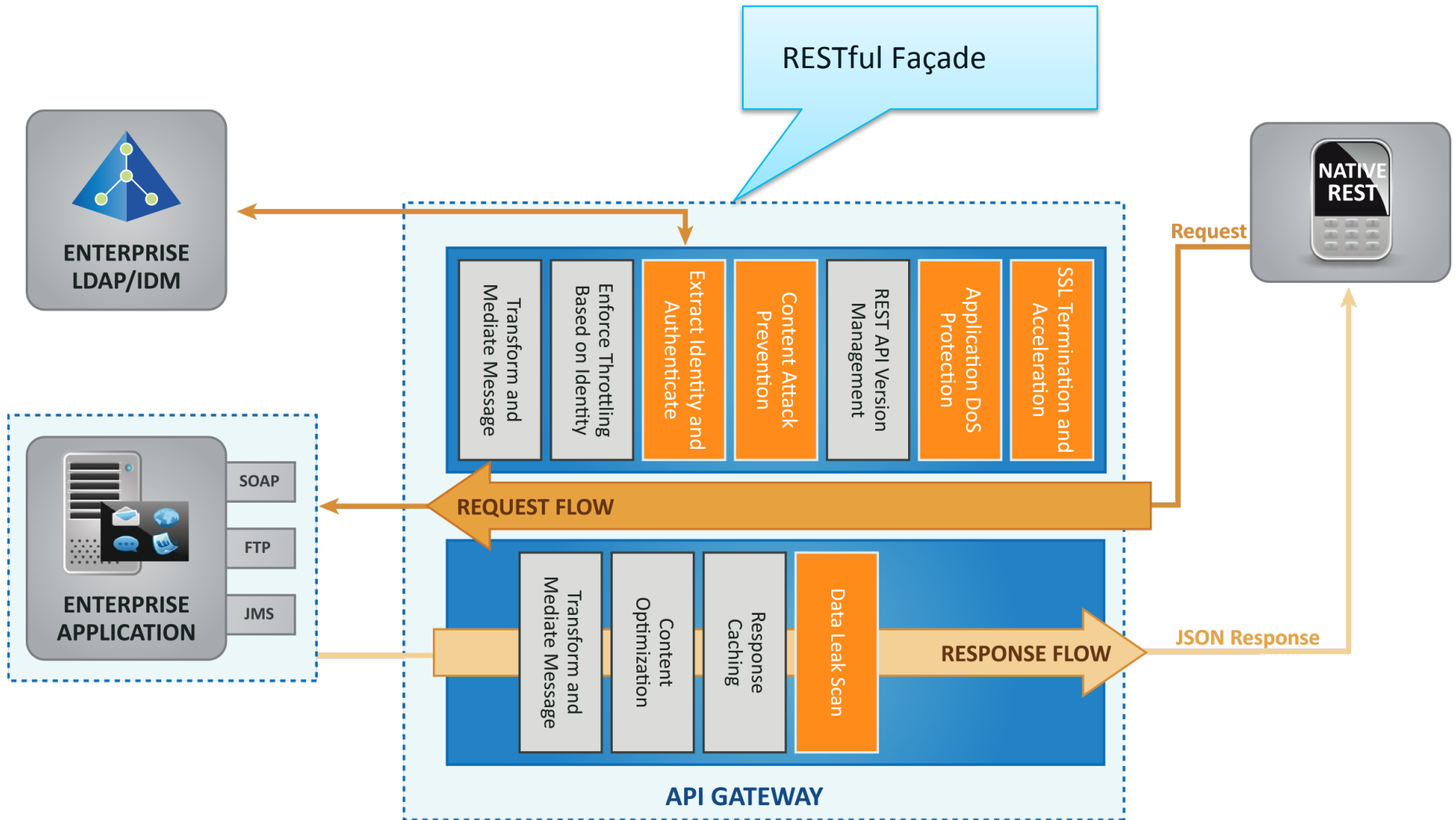*"...except for the problem of too many layers of indirection." – Kevlin Henny*

REST API Façade: Security Processing Flow

Building the App - Architecture

API Communication
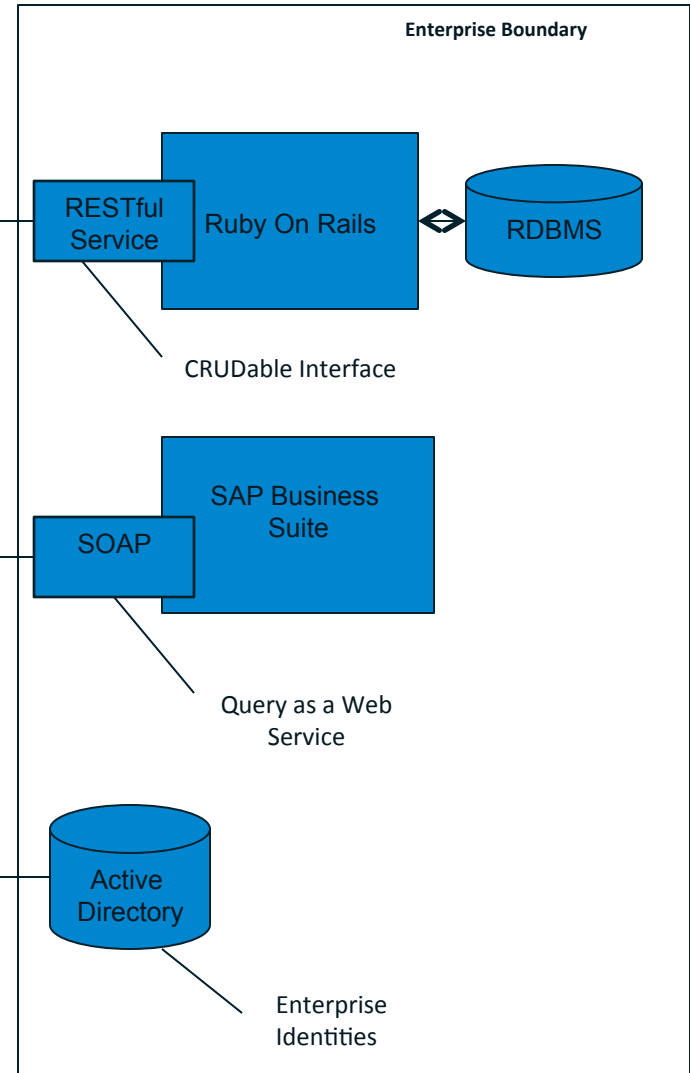
Service Gateway

Enterprise Boundary

RESTful Service

Ruby On Rails

RDBMS

CRUDable Interface

SOAP

SAP Business Suite

Query as a Web Service

Active Directory

Enterprise Identities

Application Requirements

- Retail Sales Manager – Uses Tablet, no Laptop

- Needs to query store revenue information
  - Store name, city, state, revenue

- Needs to post new hire PII information
  - Name, address, phone number, SSN, drivers license #

(intel)

Case Study (BCBSA) API
Integration & Security Brokerage

Users also enter reviews/ data into Portal

Browser or
Mobile
AuthN /Info
Request

Goal: Transparent patient healthcare cost info available on mobile devices available to member organizations

Problem: Point to point integration costs, poor scalability, fragmented data for Member Consumers

Solution: Security Brokerage with consistent, managed API using a service gateway

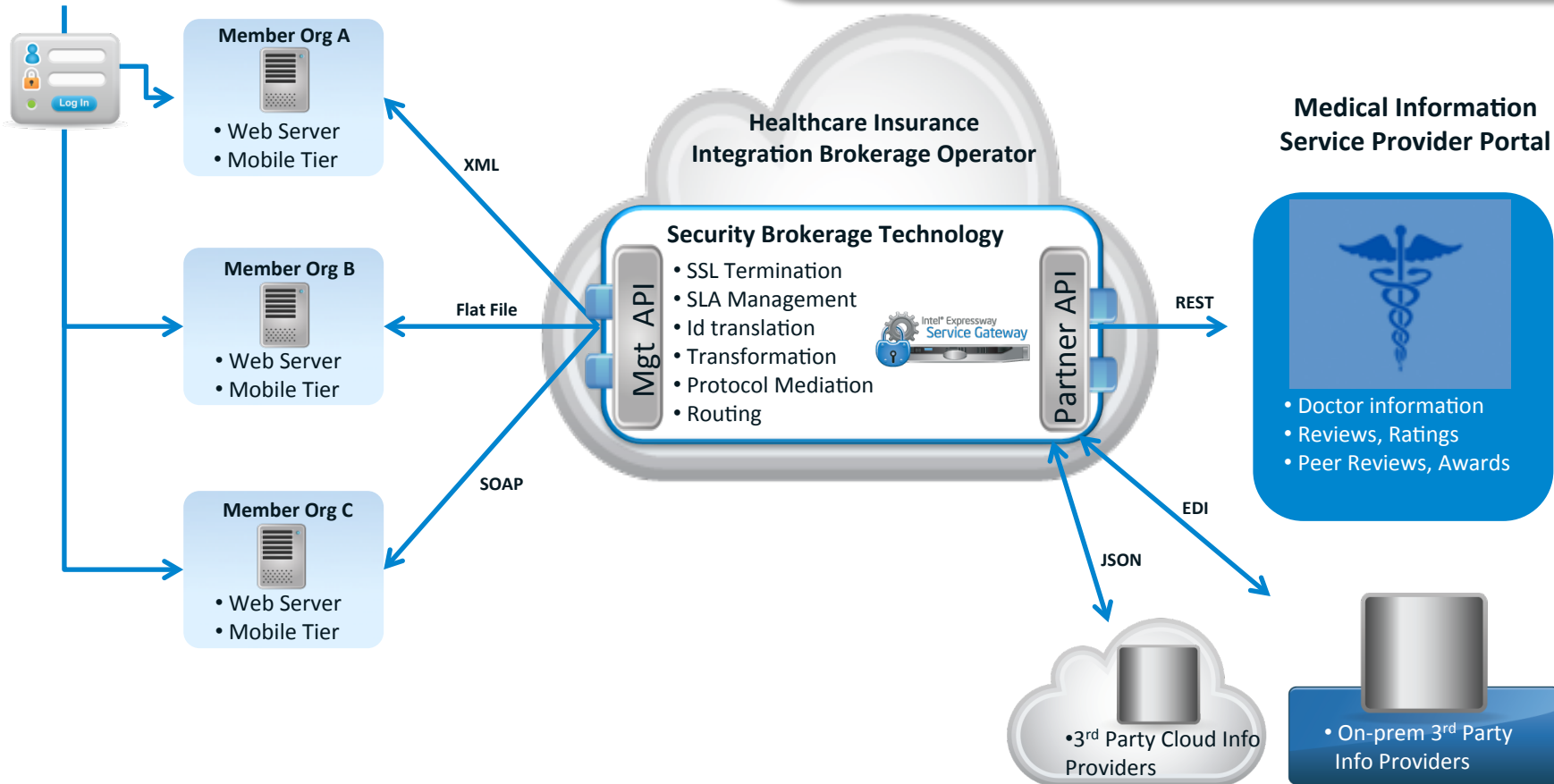**Member Org A**
- Web Server
- Mobile Tier

Member Org B
- Web Server
- Mobile Tier

Member Org C
- Web Server
- Mobile Tier

XML

Flat File

SOAP

**Healthcare Insurance
Integration Brokerage Operator**

Mgt API

Security Brokerage Technology
- SSL Termination
- SLA Management
- Id translation
- Transformation
- Protocol Mediation
- Routing

Intel® Expressway
Service Gateway

Partner API

REST

**Medical Information
Service Provider Portal**

- Doctor information
- Reviews, Ratings
- Peer Reviews, Awards

JSON

EDI

- 3rd Party Cloud Info Providers

- On-prem 3rd Party Info Providers

(intel)

Example: Generic Mobile Workflow using Service Designer

SampleProcess

Palette

- Receive_REST_Call → **Receive RESTful Call**
- ContentAttackPrevention → **Scan for incoming threats**
- Extract_Identity_and_Authenticate → **Extract identity and auth**
- SLA_Enforcement → **Identity based SLA enforcement**
- Message_Transformation → **REST to SOAP (or other)**
- Invoke_Internal_Service → **Call "real" service**
- Tokenize_Response → **Tokenize or redact portions of response**
- Content_Optimization → **Compress and JSON transformation**
- Reply / McAfeeDataLossPrevention → **Final DLP check before return to mobile client**

Selection Tool

Reliable Delivery

Security

AAA

Use an AAA policy to
authenticate digital

Transformations

A/V and Malware Protection

Control

Faults

Zoom In

Zoom Out

(intel)

Example: API Authentication with OAuth

Identity Management

☑ **Extract Identity**

Identity source: `Token from HTTP OAuth Authorization ▼`

Token from HTTP OAuth Authorization details

Token type: `Bearer ▼`

Receive token type: `JSON Web Token ▼`

JSON Web Token Details

☑ Verify JSON web token signature

Signature algorithm: ☑ HMAC with SHA-256   ☑ HMAC with SHA-384   ☑ HMAC with SHA-512

Symmetric key: `Object name from incoming token ▼`

Authentication policy: `test-auth`

☐ Verify OAuth token

☐ Specify web token content locations

☐ Check uniqueness

Exception handling data (packaged in thrown fault):

HTTP status code: `401-Unauthorized ▼`

Realm:

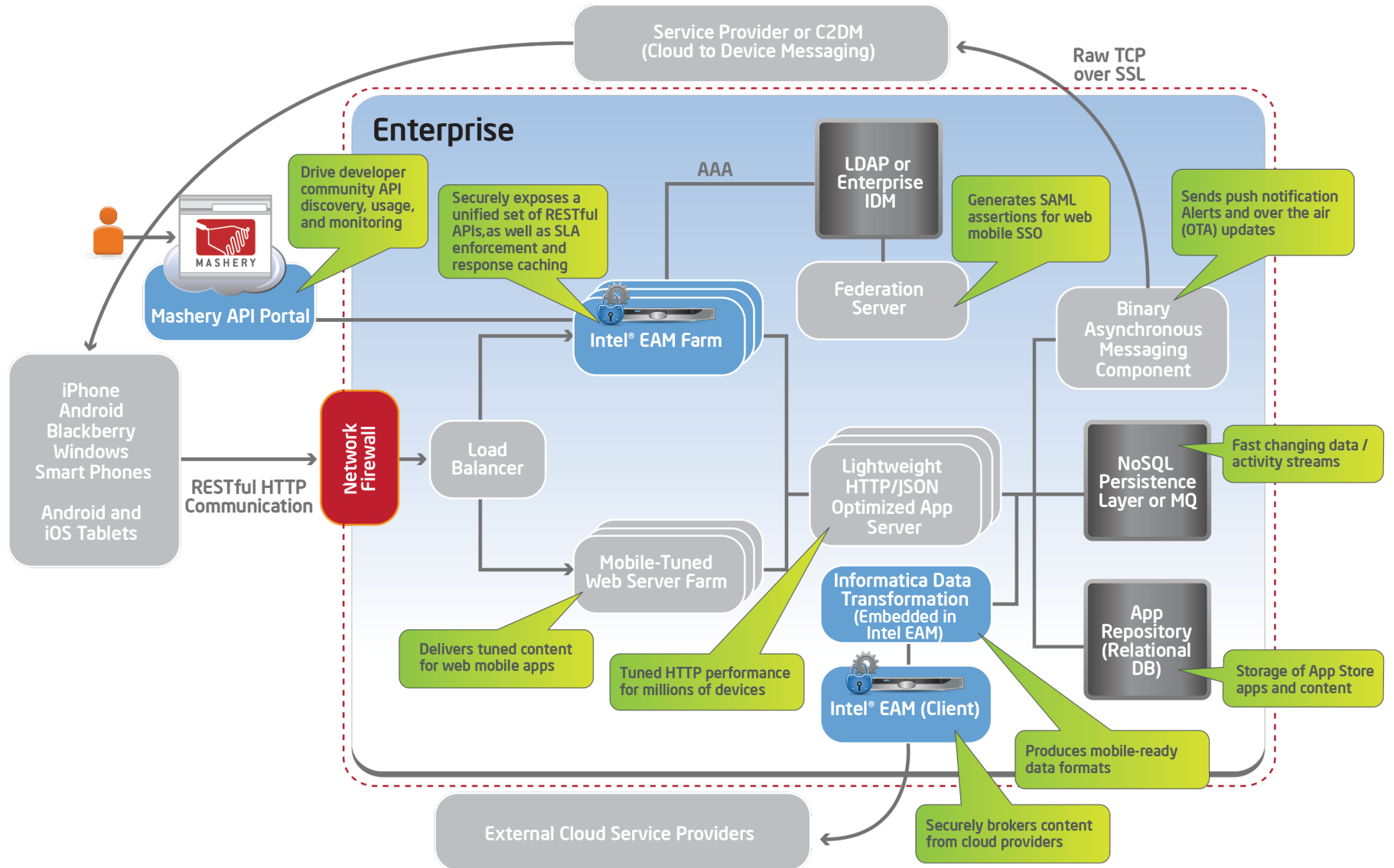⦿ Static value   ◯ Input from workflow
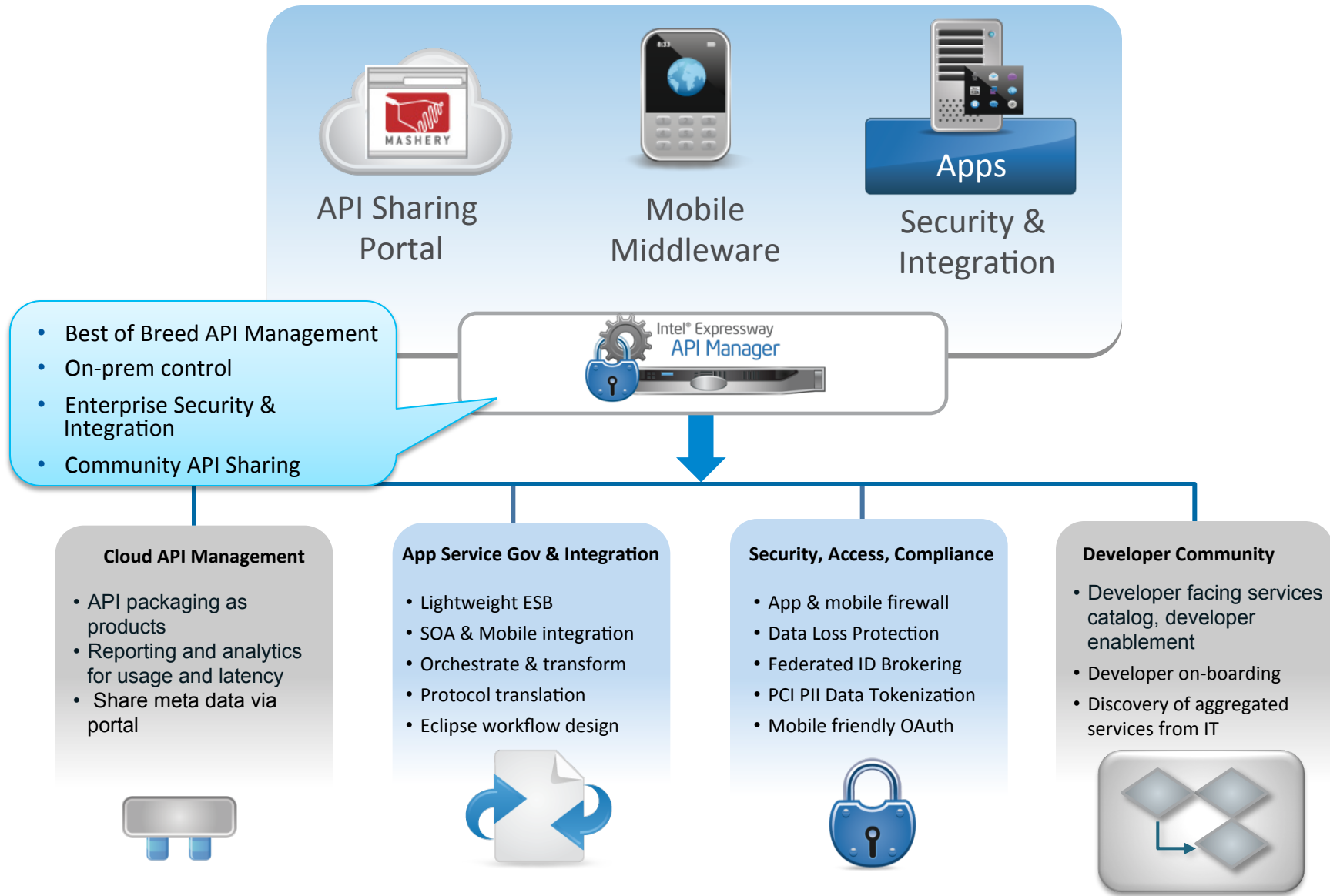
URI: `_____`

☐ Check for access token revocation

Policy-Driven Security
- Reduces coding
- Improves consistency
- Centralizes policies
- Improves security
- Enterprise grade

16

(intel)

Pulling it all Together: Ref Arch for Mobility

Service Provider or C2DM (Cloud to Device Messaging)

Raw TCP over SSL

Enterprise

LDAP or Enterprise IDM

AAA

Drive developer community API discovery, usage, and monitoring

Securely exposes a unified set of RESTful APIs, as well as SLA enforcement and response caching

Generates SAML assertions for web mobile SSO

Sends push notification Alerts and over the air (OTA) updates

MASHERY

Mashery API Portal

Intel® EAM Farm

Federation Server

Binary Asynchronous Messaging Component

iPhone Android Blackberry Windows Smart Phones

Android and iOS Tablets

RESTful HTTP Communication

Network Firewall

Load Balancer

Lightweight HTTP/JSON Optimized App Server

NoSQL Persistence Layer or MQ

Fast changing data / activity streams

Mobile-Tuned Web Server Farm

Informatica Data Transformation (Embedded in Intel EAM)

App Repository (Relational DB)

Delivers tuned content for web mobile apps

Tuned HTTP performance for millions of devices

Intel® EAM (Client)

Storage of App Store apps and content

Produces mobile-ready data formats

External Cloud Service Providers

Securely brokers content from cloud providers

17

(intel)

Intel® Expressway API Manager

API Sharing Portal

Mobile Middleware

Apps

Security & Integration

Intel® Expressway API Manager

- Best of Breed API Management
- On-prem control
- Enterprise Security & Integration
- Community API Sharing

Cloud API Management

- API packaging as products
- Reporting and analytics for usage and latency
- Share meta data via portal

App Service Gov & Integration

- Lightweight ESB
- SOA & Mobile integration
- Orchestrate & transform
- Protocol translation
- Eclipse workflow design

Security, Access, Compliance

- App & mobile firewall
- Data Loss Protection
- Federated ID Brokering
- PCI PII Data Tokenization
- Mobile friendly OAuth

Developer Community

- Developer facing services catalog, developer enablement
- Developer on-boarding
- Discovery of aggregated services from IT

(intel)

More: www.cloudsecurity.intel.com

Data Sheets & Solution Briefs

API Patterns
White Paper

Booth Drawing
$200 Virtual keypad

Composite Architecture

Composite API Platform

API Meta Data

Intel API Management Portal

- API Product Management
- Developer On-boarding
- Portal Administration
- Reporting and Analytics
- Monetization Data
- Developer Facing Service Catalog
- Developer Enablement Tools
- Admin Tools
- Community Tools
- API and Method Packaging

Powered by

MASHERY

- Service Orchestration and Composition
- Authentication and Access Control
- Authorization
- Data Format Mediation
- Protocol Mediation
- Content Attack Prevention
- SLA Management, Rate Limiting
- Lightweight ESB

(intel)

API Descriptions and Enablement Tools

Developer Community

RESTful API Consumption (from devices partners)

RESTful Façade

Service #1

Service #2

Service #3

Service Administrator

Service Developer

Intel® Expressway **API Manager**

Internal RESTful Services

Mobile Middleware (JSON/REST)

SOAP Web Services

Legacy Services (JMS, FTP, Custom, Mainframe)

Database (JDBC, HBase)

External PaaS APIs

20

(intel)