

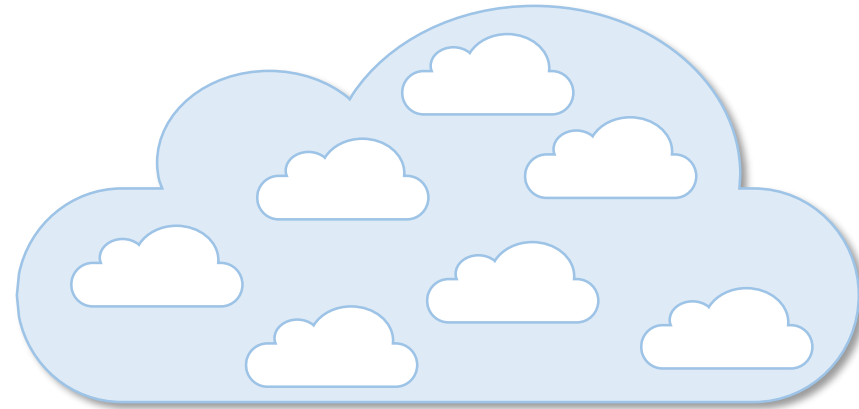
OSIsoft Cloud Services Security

Mike Lemley
Security Architect, OSIsoft



OSIsoft Cloud Services Overview

- Managed, secure, multi-tenant data platform
- Operated & maintained by  **OSI**soft.
- High speed, scalable, elastic data ingress
- Flexible, resilient, data storage
- Modern, secure REST APIs
- Built and deployed on  **Microsoft Azure**



cloud.osisoft.com

Cloud Services

G1, 2nd Floor

16:35 - 17:15



Laurent Garrigues
Strategic Product Manager
OSIssoft



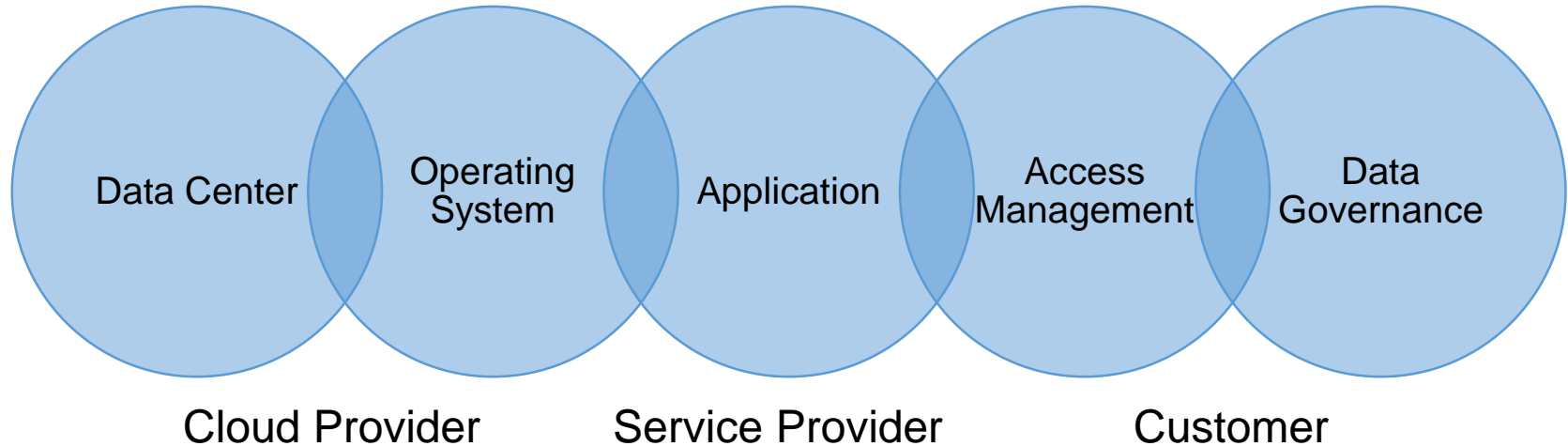
Janelle Minich
Technical Product Manager
OSIssoft



Elizabeth McErlean
Strategic Product Manager
OSIssoft

OCS as a supply chain security advantage

You can shift from needing to control everything yourself to sharing responsibility.



OCS Trust Center

OSISOFT Cloud Services

Laurent Garrigues OSISOFT Events

Trust Center

> Overview

> Identities


> Development & Operating Procedures

> Validation & Audit

> Third Parties

> Data Privacy

> Data Ownership



Overview

OSISOFT Cloud Services (OCS) provides a comprehensive and secure cloud native set of offerings for capturing, processing and sharing operational data, both within and outside of your enterprise. Because security is often a major concern with cloud-based platforms, the following sections provide an overview of OCS architecture and operations, including security controls, practices, and terminology. Each section also includes a list of Frequently Asked Questions (FAQ) on the topic addressed.

Security by Design

Because OSISOFT products and services support companies with critical infrastructure missions that require a higher standard of care than consumers and enterprise solutions, OSISOFT is committed to:

1. high-quality software
2. operational security assurance
3. clear communication about attendant risk and responsibility


OSISOFT follows the Microsoft Security Development Lifecycle methodology and OWASP practices for secure Web applications. Our commitment to improving the OCS platform is ongoing, and each update intends to raise the quality and security bar even further.

Transparency


OSISOFT's Ethical Disclosure Policy addresses transparency for issues affecting OSISOFT products and services that might appear over time. Procedures for vulnerability disclosure and handling are consistent with industry standards such as ISO 29147 and ISO 30111 respectively.

Mutual Responsibility

OSISOFT Cloud Services operate based on a shared responsibility model. OSISOFT offers a platform to its customers, operating it in a way that can meet customer's security and compliance needs. To fulfill those needs, customers are also responsible for using this platform in a way that is compliant with their security policies and regulatory constraints.



© 2017-2019 - OSISOFT, LLC.



Case Study



Australian Government
Australian Signals Directorate

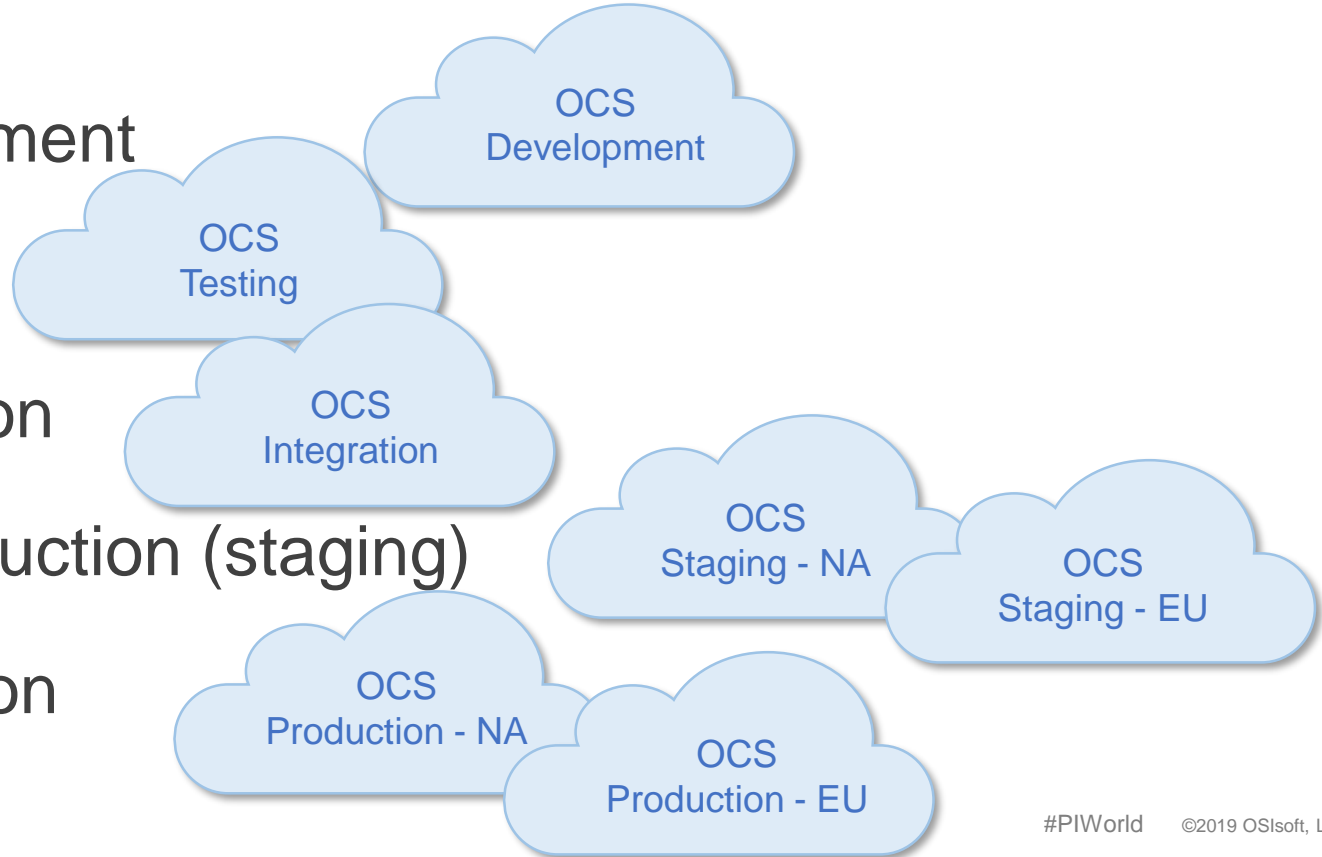
Australian Government “Essential Eight”	On-prem	OCS
1. Application Whitelisting	Customer	OSIsoft
2. Patching applications	Customer	OSIsoft
3. Microsoft Office macro settings	Customer	Customer
4. User Application Hardening	Customer	Shared
5. Restricting administrative privileges	Customer	Shared
6. Patching operating systems	Customer	Microsoft
7. Multi-factor authentication	Customer	Customer
8. Daily backups	Customer	OSIsoft

How to tackle?

- Consistent, reliable configuration
- Reliable updates (undoable)
- Continuous Testing
- Reliable data

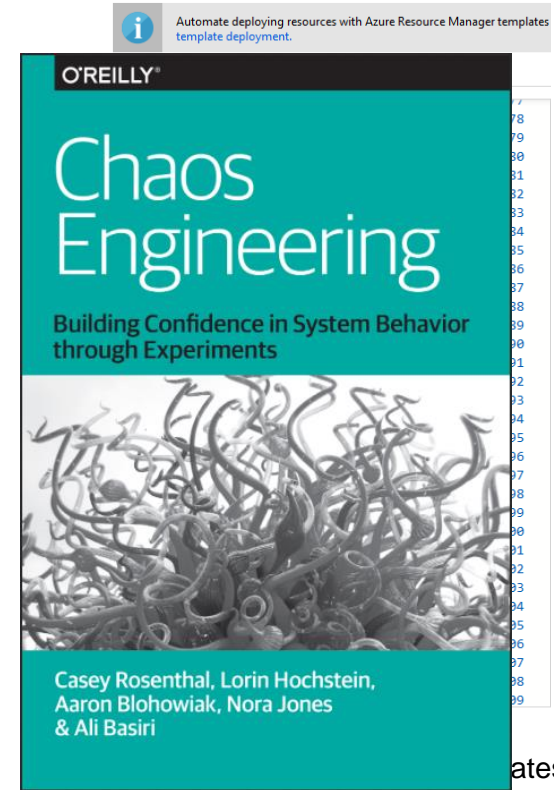
Deployment Environments

- Development
- Testing
- Integration
- Pre-production (staging)
- Production



Deployment Environment Benefits

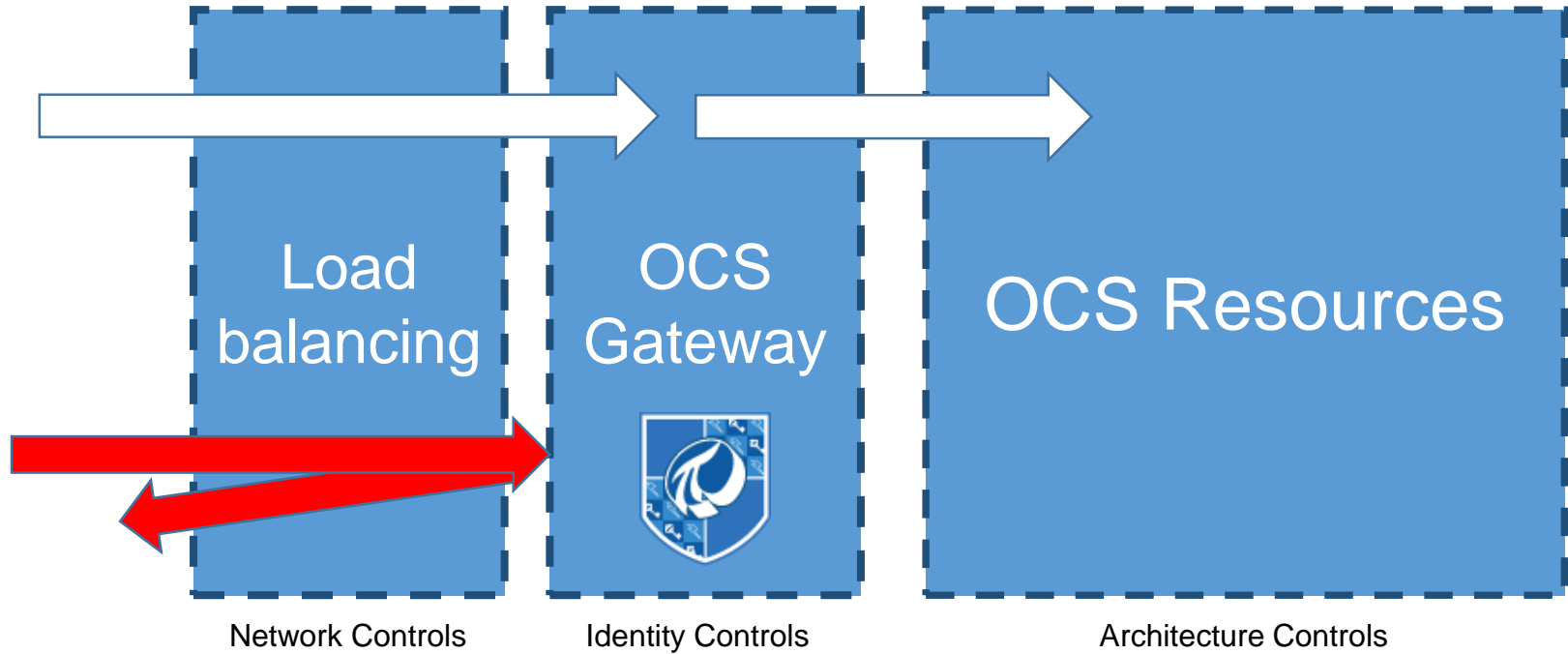
- Configuration as Code
 - [xxx] Environment = Production Environment
 - Why did it fail in production?
 - Eliminate manual configuration mistakes
- Continuous Updates & Rollback
 - O/S Updates
 - Software patches
- Continuous Testing
- Monitored & Analyzed
- Highly available, distributed databases



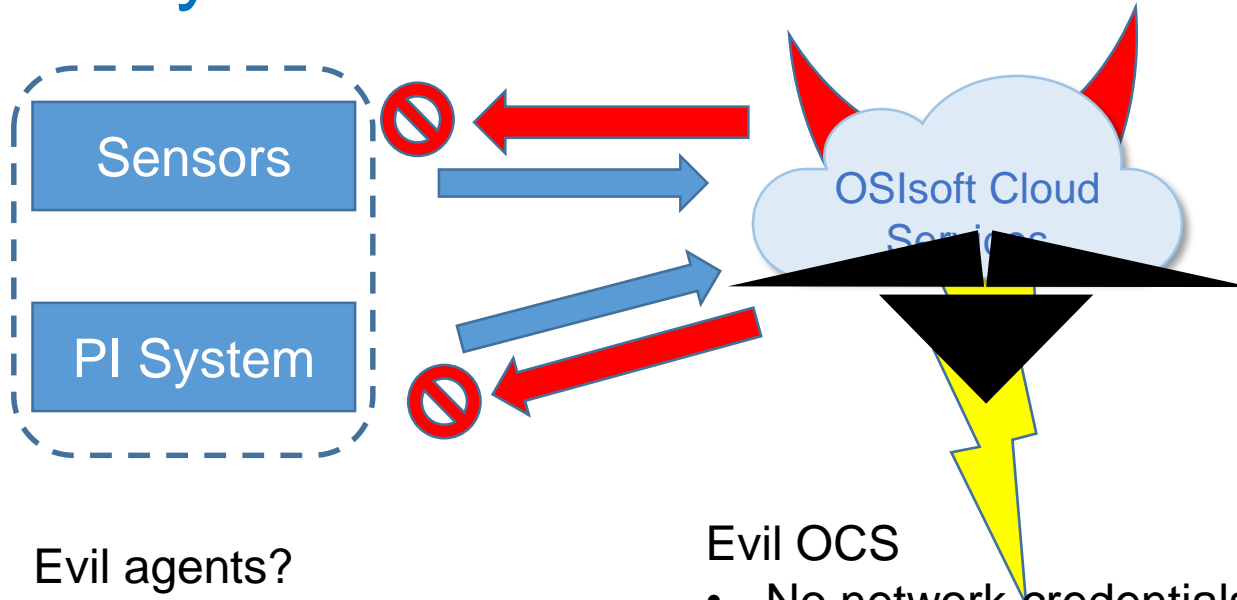
Is my data available?

- Distributed Denial of Service protection
- Scalable architecture
 - Increases resources
 - Meets peak demands

OCS Gateway



Is my network safe?



Evil agents?

- Low privilege
- OSIsoft signed

Evil OCS

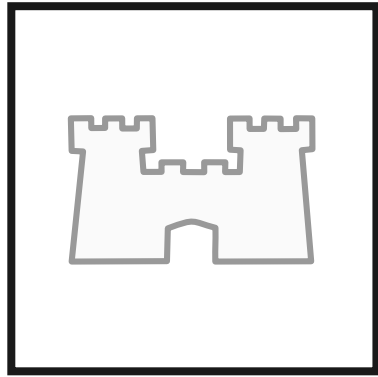
- No network credentials
- No execution on your network

Is my data safe?

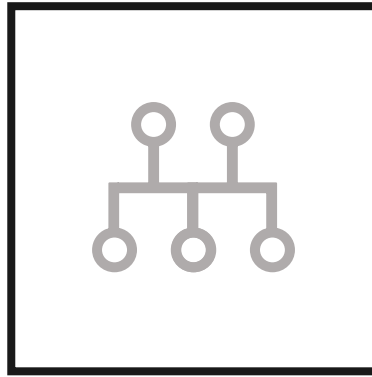
Theft and Tampering

- Support latest identity standards
- You control authentication
- Architect to leverage the evolving identity industry
- Encrypted at rest

Evolution of Security Perimeters



Physical

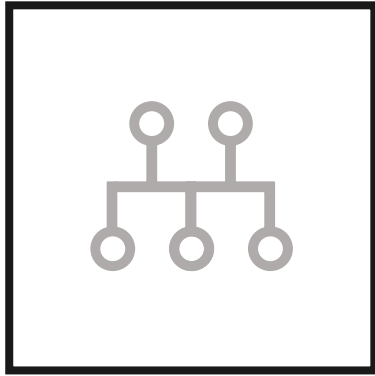


Network



Identity

Identity as the primary OCS security perimeter



Network

Network security protects against classic attacks...

...but is bypassed reliably

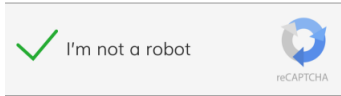
- Phishing
- Credential theft

A strong **Identity security perimeter** is critical for OCS

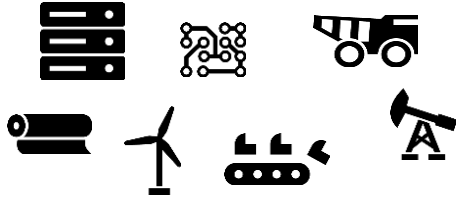
- Built on OpenID Connect/OAuth 2.0

Different Identity types

- Humans – Interactive



- Machines – Silent



Human Identity – Authenticated by your IdP

- Multi-factor authentication
- IP address
- Location/geo-fencing
- FIDO 2
- Threat Intelligence challenges

Human Identity - IdP Supported by OCS

- Microsoft Azure Active Directory




- Google



- Microsoft Live



Machine Identity

-  OpenID[®] Connect client ID and secret.
- Theft protections/defenses
 - HTTPS only
 - Credential revocation
 - clientID has limited access
 - No access to your network
 - Secret expiration
 - Secret: 32 byte (256 bit) cryptographically random

Time to crack a password

Password Length	Time to Crack	... with special character
9 characters	2 minutes	2 hours
10 characters	2 hours	1 week
11 characters	6 days	2 years
12 characters	1 year	2 centuries
13 characters	64 years	—

Source Jeff Atwood, April 2015

<https://blog.codinghorror.com/your-password-is-too-damn-short/>

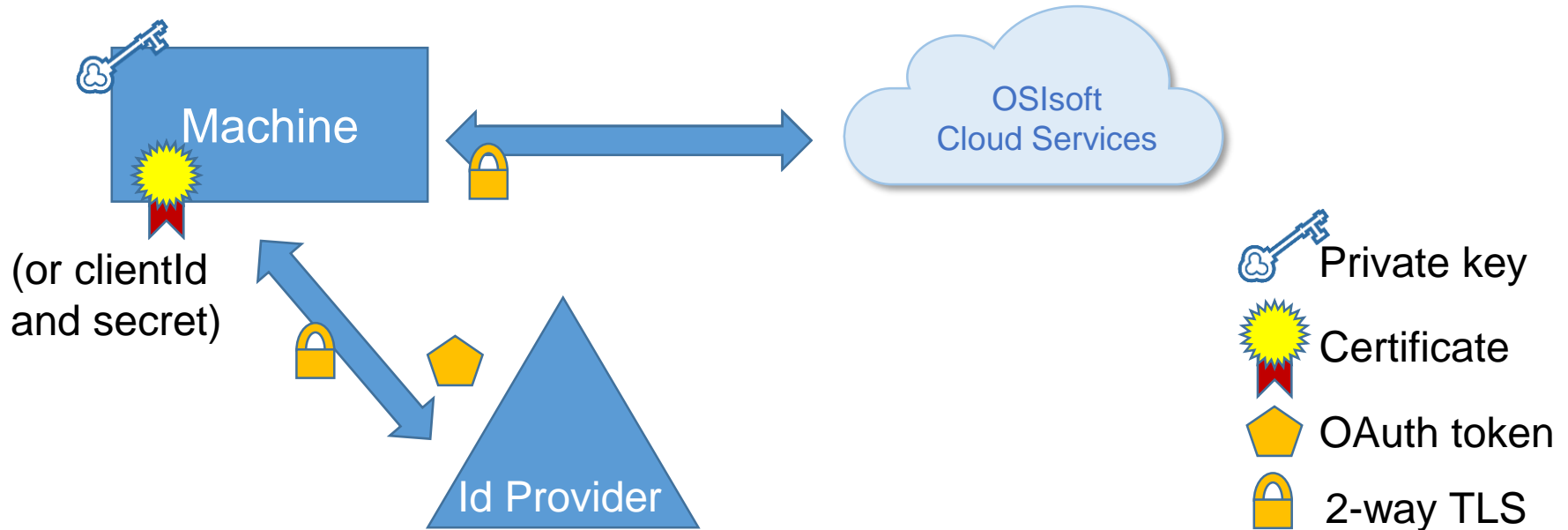
Machine Identity Challenges

- Industry less mature (than human identity)
- Credential rotation
- On-boarding/provisioning identity
- Labor intensive
- Admin credentials required
- Doesn't scale to provisioning 100's of devices
- Private Key Infrastructure (PKI) challenges

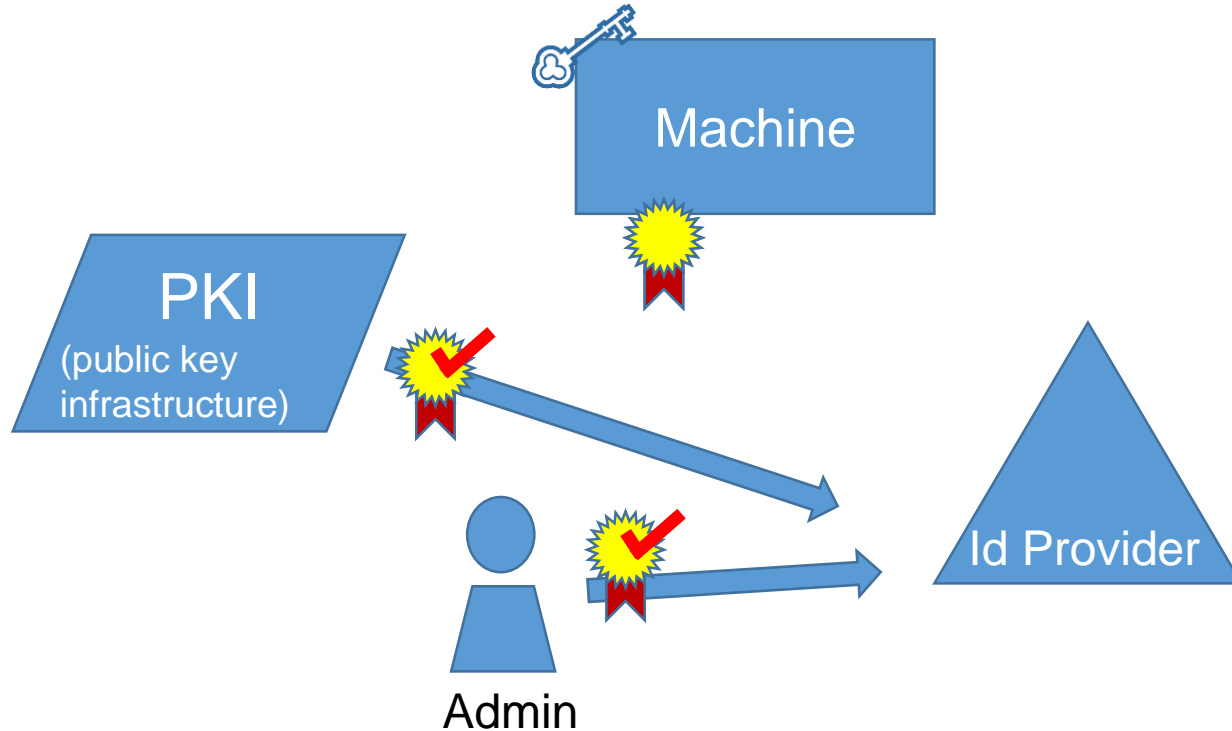
Mike's Crystal Ball – using standards

- Devices/machines
 - Self-register
 - Rotate their credentials
 - Support self-certificate authentication
 - Support manufacture provisioned certificate auth
- Support Your ID Provider for device identity
 - Leverage industry identity experts

Mike's Crystal Ball – the glue is OAuth tokens



Mike's Crystal Ball – Provisioning using standards



Mike's Crystal Ball – Federation standards

- WS-Federation
- SAML
- OpenID Connect



Mike's Crystal Ball For the Standards Geeks

- OAuth 2.0 Dynamic Client Registration (IETF RFC 7591)
- OAuth 2.0 Dynamic Client Registration Management (IETF RFC 7592)
- OAuth 2.0 Mutual TLS and Certificate Bound Access Tokens (IETF draft)
- Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs) (IETF RFC 7800)



Security Development Lifecycle (SDL)

- Dynamic Scanning

- Qualys
- SSL Labs
- BitSight



Qualys®

BIT SIGHT
The Standard in SECURITY RATINGS

- Fuzzing

- Microsoft Security Risk Detection



Microsoft

- Static Analysis Security Tool

- Synopsys Coverity



coverity™
a higher code™

- Software Component Analysis

- Synopsys Black Duck



BLACK DUCK

- Penetration testing

- OSIssoft development best practices

IOActive®



Summary

- Fundamental Security advantages
- Identity is the new perimeter
- Leverage your Identity Access Management
- Share your identity plans
 - Cloud Services or PI System
 - Understand your plans for IAM
 - What Identity Provider do you use?

OCS Security



- Mike Lemley
- Security Architect
- OSIsoft
- mlemley@osisoft.com

Questions?

Please wait for
the **microphone**

State your
name & company



Please remember to...

Complete the Survey!

Navigate to this session in
the mobile app for survey

