

Design Round-Table –
Internet of Things
Risk and Security Design

Mats Göthe
Senior Design Lead
Watson IoT Platform

Victoria Paterson
Senior Design Lead
Watson IoT Platform

InterConnect
2017



Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

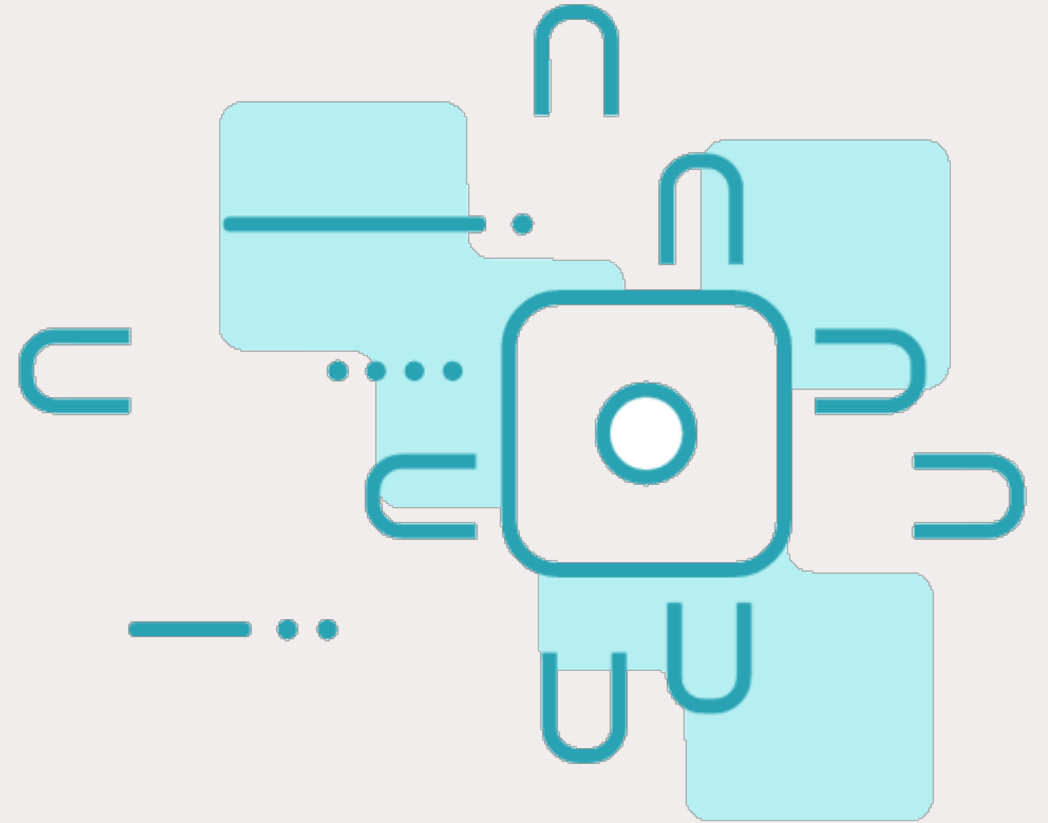
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Abstract

The Watson IoT Platform design puts users first in researching your usage patterns, use cases and needs.

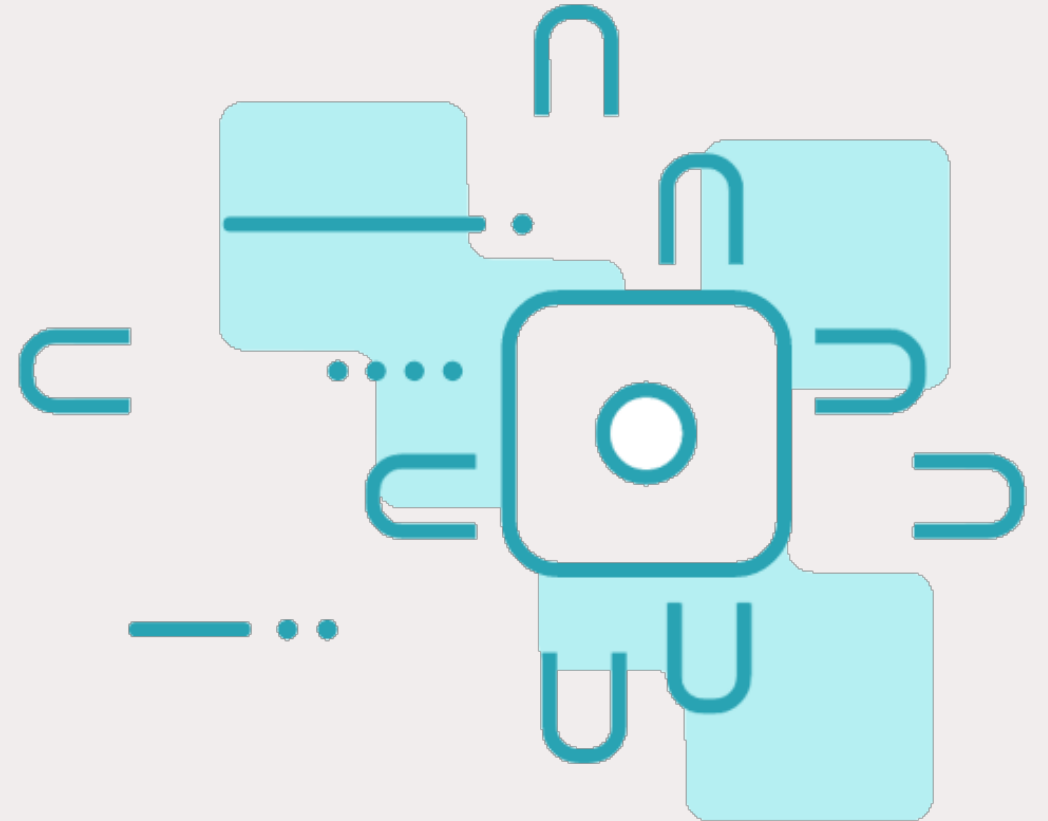
This roundtable session will present and discuss the IoT Platform Risk and Security Management experience.

Share your insights, needs, wants and requests for managing risk and security on devices and things in the IBM Watson Internet of Things Platform!



Agenda

- Introductions
- Discussion topics
- IoT Security Management - Policies
(Tuesday March 21th)
- IoT Security Management - Access Control
(Wednesday March 22th)
- Summary and conclusions
- How to engage
with Watson IoT Platform Design



Introduktions

- “Hi, I’m Mats, Design Lead for the IBM Watson IoT Platform”

Who are you?

- Your name
- Your company
- Your role



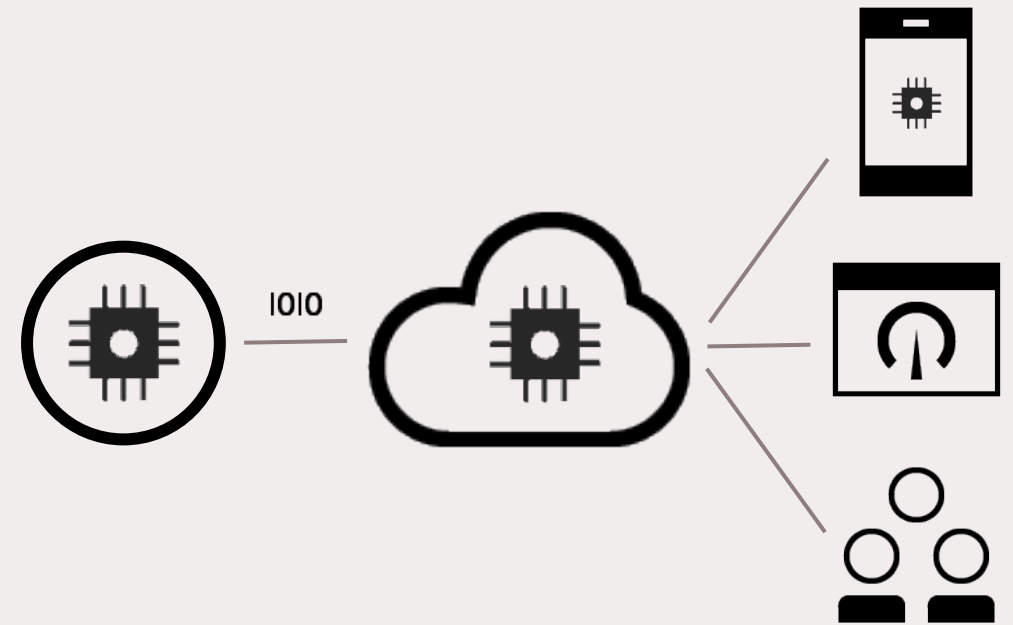
IoT Security Management - Policies

What is Watson IoT Platform?

The IBM Watson Internet of Things Platform is a fully managed cloud-hosted service available in IBM Bluemix.

Devices connects and sends IoT data securely to the IBM Watson IoT Platform service using the MQTT messaging protocol.

From there, devices are managed using your online dashboard or secure APIs, so that IoT solutions and applications can access real-time device state and historical IoT data.

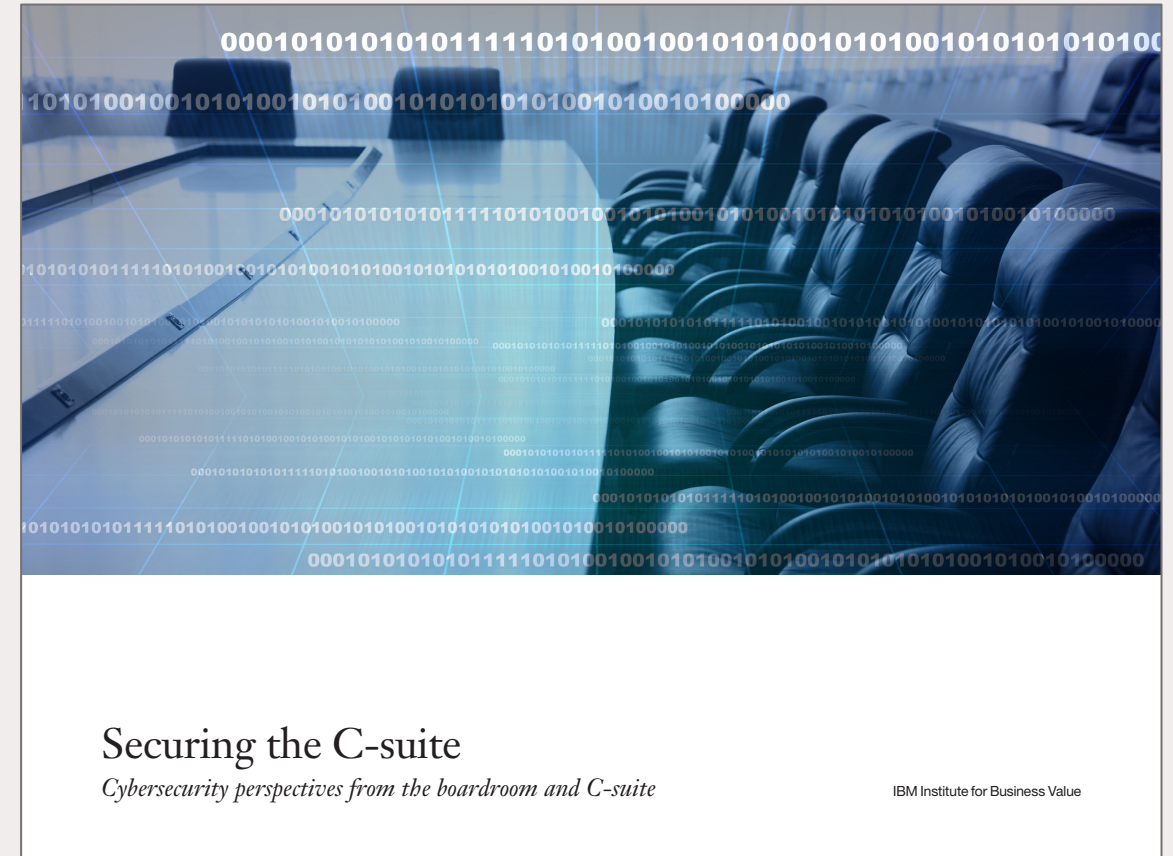


Your IoT Security Risks

“Ninety-four percent of CxOs believe it is probable their companies will experience a significant cybersecurity incident in the next two years”

“An effective tactic to combat cybercrime is transparency and collaboration, sharing incident information”

“improve awareness and drive a more risk-aware culture across the entire organization.”



Discussion - Your IoT Security Risks

- What are your IoT solution security risks today?
- What are your IoT security KPIs?
- How do you monitor and report on risk and security compliance?



What is Risk and Security Management?

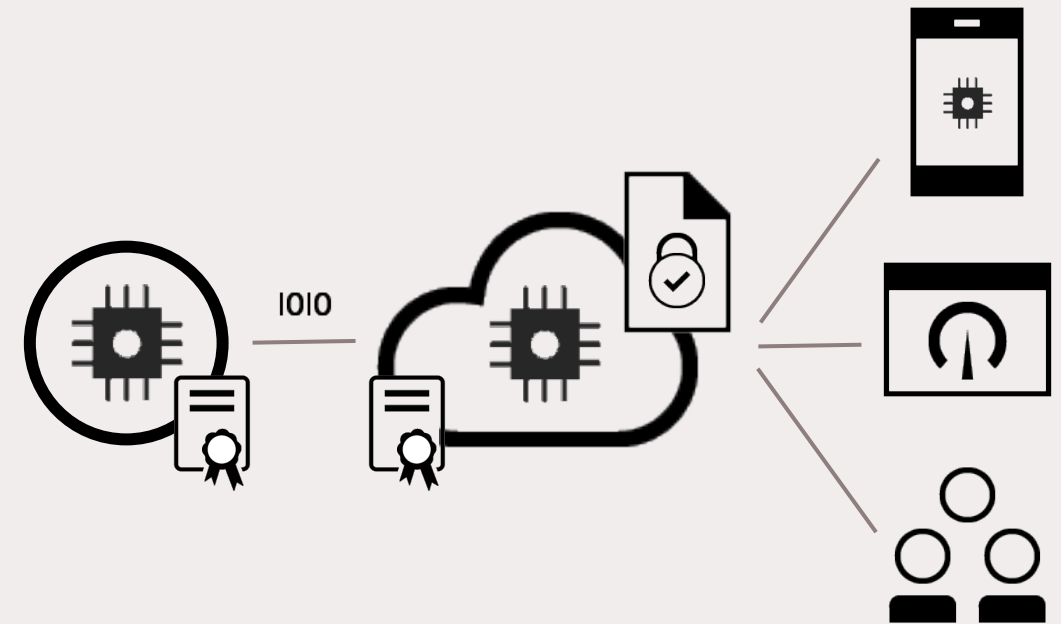
IoT Platform Risk and Security Management to manage risk and gather insights across your entire IoT landscape using policies, dashboards, reports and alerts.

IoT Security Management provides **connection security policies** using client and server certificates and TLS authentication.

Risk and Security Management provides policies to **blacklist or whitelist devices** through IP addresses, ranges or geographies.

Risk and Security Management provides policies on **device health**

Risk and Security Management provides **drill-in reports** to act on detected risks and device anomalies.



Risk and Security Management Policies

Additions in the IoT Platform UI to create, view and manage IoT Security Policies.

- **Connection Security Policy view** of connection security levels
- **Blacklist / Whitelist Policy view** of blocked IP addresses
- **Risk and Security Dashboard** with summary KPIs on policies
- **Certificates** on device clients and IoT server



Discussion – Risk and Security Management Policies

- Do you agree or disagree with the usefulness of the Connection Security Policy
- What IoT Security Policies and KPIs are you missing?



Discussion – Risk and Security Management Policies

- Rank the importance of the Security Policies
 - Device Connection Security
 - Blacklist and Whitelist
 - Device Connection Health
 - Firmware Version
 - Gateway rules on device connections
 - Geofencing
 - Device Behavior Anomalies



Working with IoT Risk and Security Policies

The screenshot shows the IBM Watson IoT Platform interface. At the top, there's a dark blue header with the text "IBM Watson IoT Platform" on the left and navigation links "QUICKSTART", "SERVICE STATUS", "DOCUMENTATION", and "BLOG" in the center. On the right of the header, a user profile is shown with the email "cynthiaz@ca.ibm.com" and ID "ID: (ke0s2h)". Below the header is a dark blue sidebar with various icons. The main content area is titled "Policies" and contains a sub-header "Policies" with a description: "You can configure policies to enhance connection security and control access to the server from devices." Below this, there are three policy cards: "Connection Security" (with a "Configure" button), "Blacklist" (with a "Disabled" status and a "Configure" button), and "Whitelist" (with a "Disabled" status and a "Configure" button).

To configure Policies

- Go to the Security section in the Navigator
- Configure the Connection Security Policy

Working with IoT Risk and Security Policies

The screenshot shows the IBM Watson IoT Platform interface. The top navigation bar includes 'QUICKSTART', 'SERVICE STATUS', 'DOCUMENTATION', and 'BLOG'. The user is logged in as 'lotlab@mail.com' with ID '01gah1'. The left sidebar contains icons for various IoT functions, with the 'Security' icon (a padlock) highlighted. The main content area is titled 'Default Connection Security' and includes a 'Back to Policies' button. It contains instructions on setting default security levels and a table of options. A 'Refresh Compliance' button is also present.

IBM Watson IoT Platform

QUICKSTART SERVICE STATUS DOCUMENTATION BLOG lotlab@mail.com ID: (01gah1)

← Back to Policies Cancel Save

Default Connection Security

Set the default security level that is applied to all devices. You can then add custom connection security for specific devices.

Specify the default connection security levels to use for all device types that are not configured separately in the Custom Connection Security section. You can view the number of devices that are affected and the predicted level of compliance.

Note: The device number and predicted compliance values are estimates based on a report that runs at varying intervals.

Default Security Level	TLS Optional
Devices in organization	TLS Optional
Devices in Default Security Level	TLS with Token Authentication
Predicted Compliance ⓘ	TLS with Client Certificate Authentication
	TLS with Client Certificate AND Token Authentication
	TLS with either Client Certificate OR Token Authentication

Refresh Compliance

Custom Connection Security

You can add custom connection security to apply different security level to specific devices. The predicted compliance value is updated to reflect the default settings and the custom settings.

To configure Policies

- Go to the Security section in the Navigator
- Configure the Connection Security Policy
- Select a Default Security Level for TLS Authentication

Working with IoT Risk and Security Policies

The screenshot displays the IBM Watson IoT Platform interface. The top navigation bar includes links for QUICKSTART, SERVICE STATUS, DOCUMENTATION, and BLOG, along with a user profile for mats.gothe@se.ibm.com. The left sidebar contains various icons for navigation. The main content area shows the 'Default Security Level' set to 'TLS with Token Authentication' and a 'Refresh Compliance' button. Below this, it indicates '20 devices' in the organization and '5 devices' in the default security level. A 'Predicted Compliance' section shows a green bar representing 4 Pass, 0 Fail, and 1 Unknown status, with a warning that the prediction has expired. The 'Custom Connection Security' section provides instructions on adding custom security levels and includes a table of existing configurations.

Device Type	Security Level	Predicted Compliance
arduino	TLS Optional	5 Pass 0 Fail 0 Unknown
intel-edison	TLS with Client Certificate Authentication	4 Pass 0 Fail 1 Unknown
intel-galileo	TLS with Client Certificate Authentication	0 Pass 4 Fail 1 Unknown

To configure Policies

- Go to the Security section in the Navigator
- Configure the Connection Security Policy
- Select a Default Security Level for TLS Authentication
- Add custom security levels, by type

Working with IoT Risk and Security Policies

The screenshot displays the IBM Watson IoT Platform interface. At the top, the header includes the logo, navigation links (QUICKSTART, SERVICE STATUS, DOCUMENTATION, BLOG), and user information (cynthiaz@ca.ibm.com, ID: (ke0s2h)). The left sidebar contains various icons for navigation. The main content area shows the 'Blacklist' section with a '+ Add to Blacklist' button. A modal dialog box titled 'Add to Blacklist' is open, prompting the user to select specific IP addresses, ranges, or countries. The dialog includes a 'Block access from:' section with tabs for 'IP Address/Range', 'CIDR', and 'Country'. A text input field contains '192.143.0.1'. Below this, examples are listed: '192.168.0.1', '192.168.0.1-192.168.0.10', '2001:0db8:85a3::8a2e:0370:7334', and '1080:0:0:8:800:200c:417a-1080:0:0:8:800:200c:417d'. A 'Comment (optional):' field contains 'Bad IP'. The dialog has 'Cancel' and 'Add' buttons at the bottom.

To configure Policies

- Go to the Security section in the Navigator
- Configure the Blacklist and Whitelist Policy
- Add IP addresses, IP ranges, or IP geographies

Working with IoT Risk and Security Policies

The screenshot shows the IBM Watson IoT Platform interface. The top navigation bar includes links for QUICKSTART, SERVICE STATUS, DOCUMENTATION, and BLOG. The user's email (mats.gothel@sa.ibm.com) and ID (InterConnect 2ufin) are displayed. The left sidebar contains various icons for navigation. The main content area is titled "CA Certificates" and includes a description: "Upload a CA certificate which is used to authenticate the signature of client-side certificates. You can enforce TLS client authentication by configuring the Risk Management Connection Security policy." Below this is a "+ Add Certificate" button. A table lists the certificates:

☐	Common Name	Issued By	Valid To	
☐	ACME Intermediate CA	ACME Root CA	13/02/2027	
☒	ACME Root CA	ACME Root CA	15/11/2026	

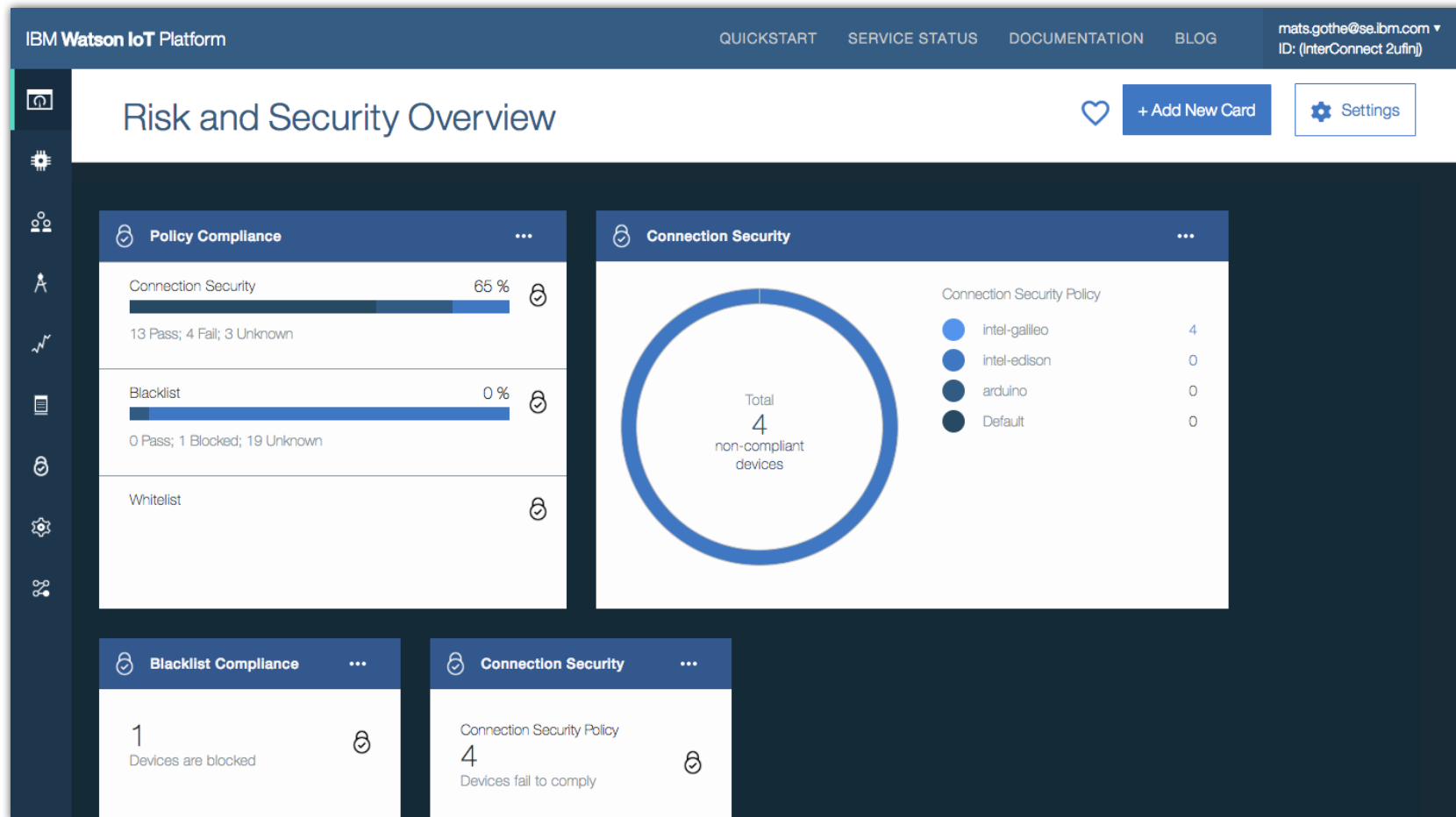
Below the table is a "Certificate Details" section for the selected "ACME Root CA":

Common Name: ACME Root CA
Issued By: ACME Root CA
Comments:
Public Key: RSA-2048
Valid From: 15/02/2017
Valid To: 15/11/2026

To configure Certificates

- Go to the Settings section in the Navigator
- Configure the CA and Server certificates
- Import a certificate to the platform
- Submit a certificate signing request (CSR)

Working with IoT Risk and Security Policies



To monitor security

- Go to the Dashboard section in the Navigator
- View security KPIs

Discussion – Working with Risk and Security Policies

- Do you agree or disagree with the usefulness of the Connection Security Policy?
- What personas in your organization would configure security policies?
- What personas in your organization would use the Risk and Security Dashboard?
- What changes would you suggest on this design?



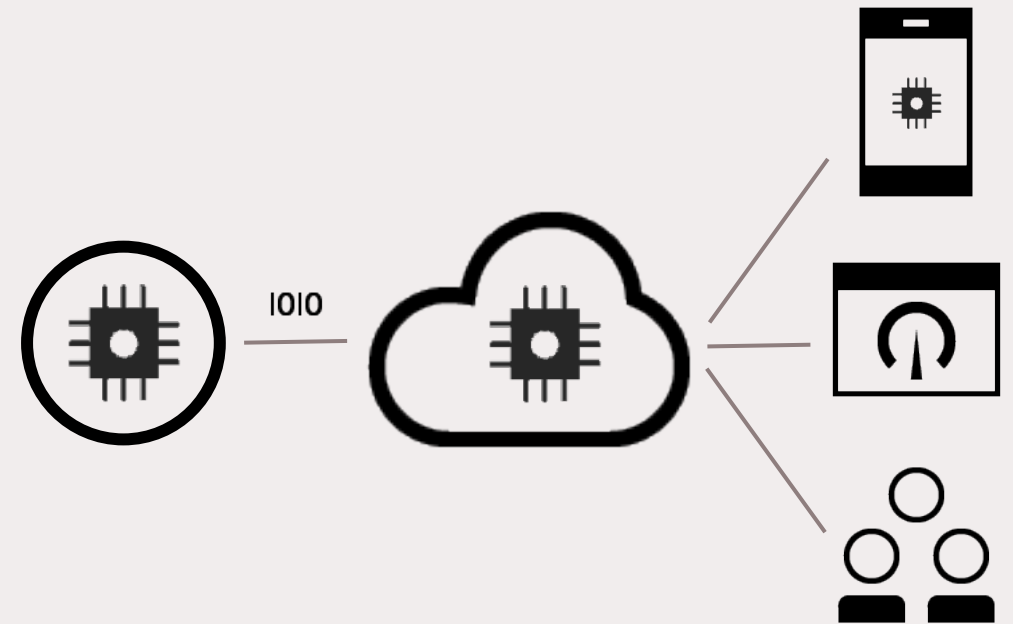
IoT Security Management - Access Control

What is Watson IoT Platform?

The IBM Watson Internet of Things Platform is a fully managed cloud-hosted service available in IBM Bluemix.

Devices connects and sends IoT data securely to the IBM Watson IoT Platform service using the MQTT messaging protocol.

From there, devices are managed using your online dashboard or secure APIs, so that IoT solutions and applications can access real-time device state and historical IoT data.



What is Watson IoT Platform Security

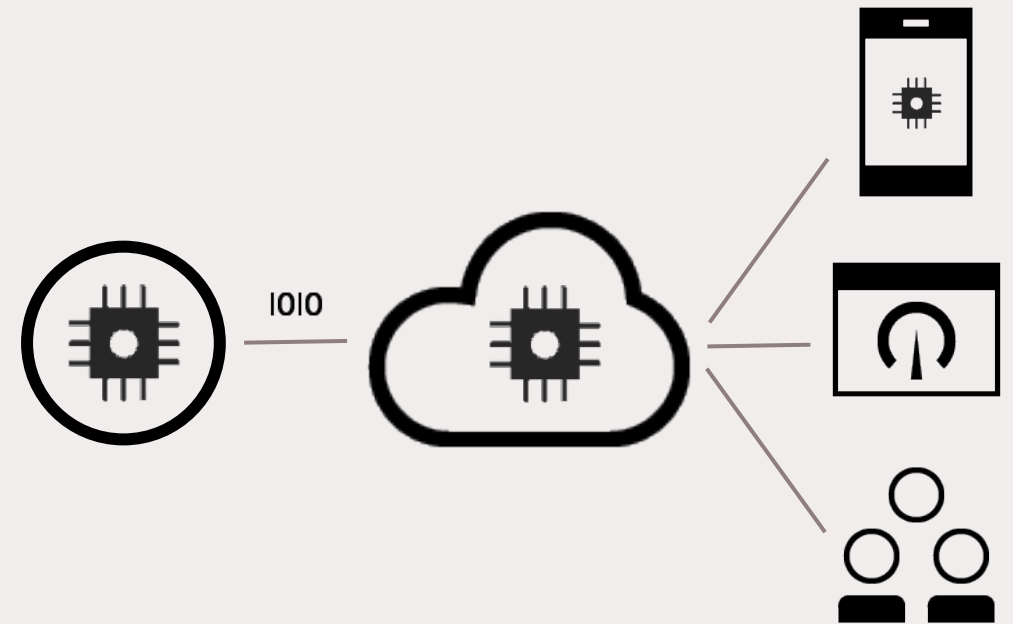
IBM Watson IoT Platform embeds security as an important aspect of its architecture

Compliance: external **standards** which set benchmarks for security

Authentication: assuring the **identity of users, devices or applications** that are attempting to access your organization's information

Authorization: assuring that users, applications and devices have **role based permission** to access IoT data and perform actions

Encryption: assuring that data is **encrypted** and only readable by authorized parties only and cannot be intercepted

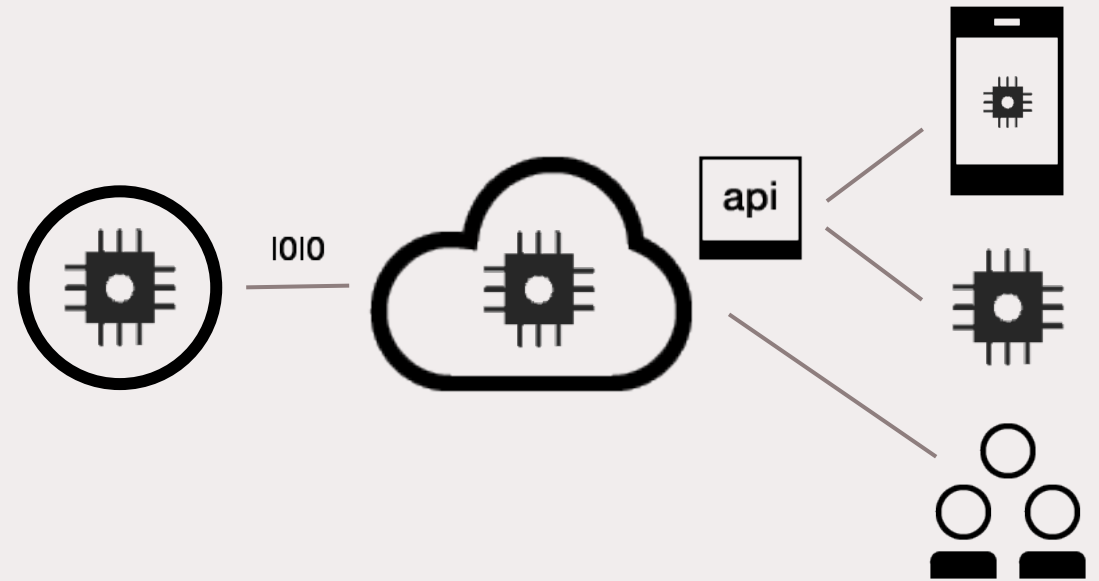


What is Member Ids and API keys

IBM Watson IoT Platform assures the identity of users, devices or applications attempting to access the IoT Platform

Access for Users to the web-based UI is authenticated by a IBMid or Bluemix Single Sign On

Access for Applications and Devices to the REST API is authenticated by an API key, generated through the UI in your IoT platform organization



Discussion – Members and API keys

- How do you manage user identities?
In the IoT Platform or in an external directory?
- How do you control distribution, usage and revocation of IoT Platform Members and API keys?
- How do you organize and track user and application identities?
- At what scale are you adding IoT Platform Members and API keys?



What is the Access Control Model?

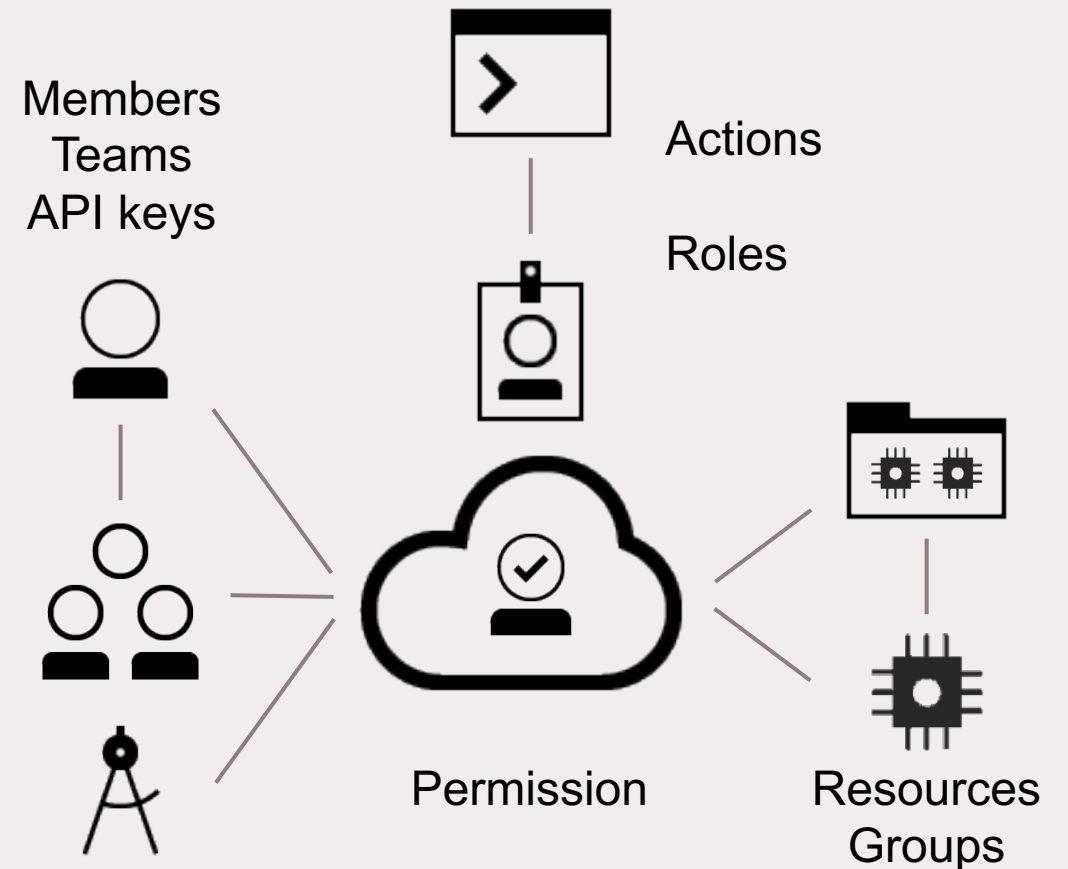
IBM Watson IoT Platform defines a **Access Control model based on Subjects, Actions and Resources**

Subjects: Members and API keys that may be grouped in Teams

Roles: Pre-defined or Custom-defined selection of Actions permitted

Resources: Groupings of resources

Permission: The permitted actions (by Role) that can be performed on selected resources (by Group)



Discussion – Resource Level Access Control

- Do you agree or disagree with the usefulness of permissions at resource level?
- Do you agree or disagree with providing permissions to resources using Groups?
- How do you manage roles, permissions and resources in groups? In the IoT Platform User Interface or through the IoT Platform APIs?
- What resource types would you prioritize for groups and resource level access control?



Discussion – Resource Level Access Control

- What resource types would you prioritize for groups and resource level access control?
 - Devices (and Things)
 - Device and Thing Interfaces w/ Properties, Events and Commands
 - Members and API keys
 - Analytic Rules and Actions
 - Risk and Security Policies and Actions
- What other Resource Level Access Control capabilities are you missing?



Summary and Conclusions

Learn more about Watson IoT Platform

- Are you visiting the Watson IoT Platform Blog to receive notifications on platform updates?
<https://developer.ibm.com/iotplatform/blog/>
- Are you enabling Experimental Features to try new platform capabilities?
- Are you participating in the IoT Platform beta programs?



Learn more about Watson IoT Platform

Learn more about IBM's point of view on the
Internet of Things

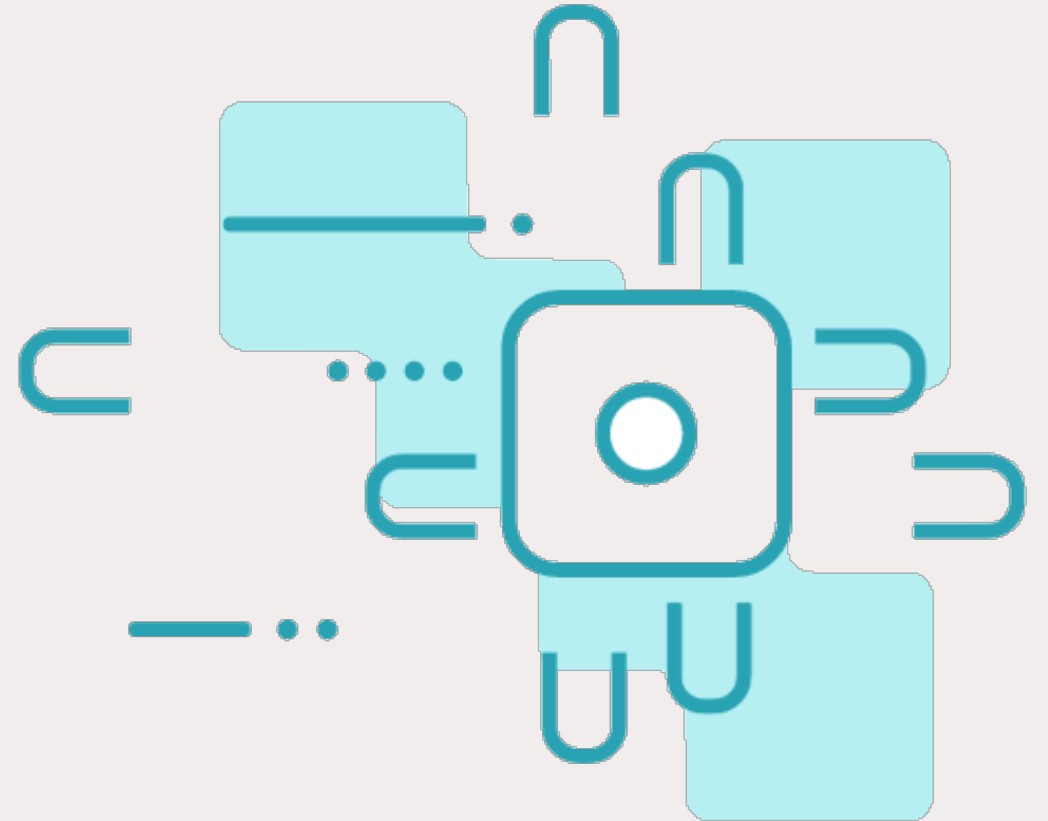
ibm.com/loT

Try out our Internet of Things platform

ibm.biz/try_iot
Bluemix.net

Join us in our IoT conversations

[@IBMIoT](https://twitter.com/IBMIoT)



Become a Design Sponsor

Join the Design Partner Program

The Watson IoT Platform Design Partner Program (DPP) is a group of selected clients and partners that are building, integrating and deploying IoT solutions using the Watson IoT Platform.

The members of the DPP are meeting monthly with IoT Platform offering management, design and development to learn about new IoT Platform capabilities in the roadmap and to provide their feedback and guidance on priorities.

Join the IoT Platform Design Partner Program



Mail us at
IOTDPP@us.ibm.com



Sign up at
<https://ibm.biz/Bds5dt>

Notices and disclaimers

Copyright © 2017 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and

the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular, purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli® Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

InterConnect 2017

