ORACLE

Cloudy with a Chance of Evaluating? Common Criteria in the Cloud—an Update on the Technical Working Group's Progress

Joshua Brickman, nominal chair CC in the Cloud TWG
Oracle Corporation
Common Criteria Day, CSfC Conference, May 9, 2022

Today's Speaker

Joshua Brickman, Senior Director Security Evaluations, Oracle Corp.

CC In the Cloud Technical Working Group

- Leads Product Security Evaluations @ Oracle
- Frequent Speaker at Security Conferences (ICCC, ICMC, RSA)
- Completed Many Security Certifications Projects since 2006

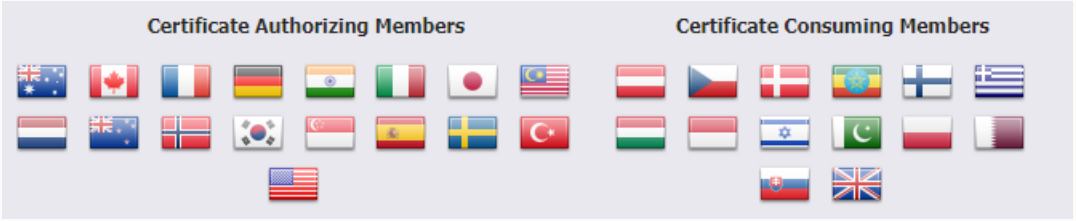
Agenda

- Why CC?
- Why CC in the Cloud?
- Why Now?
- Technical Working Group Progress
- Plans Going Forward

CC Recognition Arrangement

31 countries of CCRA

CCRA is essential for product vendors



CCRA does not exist for Cloud Authorization "Schemes”

USA

Germany and France

Spain

UK

India

China

EU Cyber Security Act

Japan-EU Partnership

EUCSA will likely create a mutually recognized cloud scheme,
but it is not clear yet that it will address “assurance”

The Move to the Cloud

- Customers are buying services, not products (April 25, 2022)
  - *"Gartner predicts that 95 per cent of new IT investments made by government agencies will be made as a service solution by 2025."*--Moving Beyond Legacy Systems (governmentnews.com)

- Cloud Security is a Priority (April 20, 2022)
  - *"The United States is working on guidance and legislation that show the government is placing increasing importance on **cloud security**. US lawmakers are working on bipartisan legislation that covers the cybersecurity responsibilities of private entities designated as "systemically important critical infrastructure." …which will require implementing certain security controls to protect their systems and for reporting cybersecurity incidents to the government.* Proposed US Guidance (securityweek.com)

Why CC in the Cloud?

- Common Criteria is an IT Product Evaluation standard. CC as defined today does not allow for evaluations in a DevOps environment where installation, configuration and administration is not managed by the customer.
- CC is the only framework that provides security assurance to ICT that is mutually recognized by 31 countries
- Therefore this technical working groups problem statement is:

There is not yet a defined and accepted method within the Common Criteria that addresses IT product evaluations in the cloud environment.

People Want CC in the Cloud but don't know how to do it

- 2019 ICCC in Singapore:
  - Mary Baish, NIAP Director listed "Evals in the Cloud" as one of their top five challenges (SaaS, PaaS, and IaaS) due to constantly changing environments.
  - Dr. Guillaume Poupart, Director General, National Cybersecurity Agency of France (ANSSI--French scheme) noted "…Cloud is on their agenda, but no real work has been done so far"
- 2021 Virtual ICCC :
  - Shantell Powell, NIAP Deputy Director listed "Evaluations in the Cloud" as one of their top five priorities in her presentation at the conference
- 2022 Common Criteria Day
  - (early questions for panel on the future of Common Criteria) "Cloud based software as a service (SaaS) management of network devices is becoming common. In fact, many commercial network devices only provide a SaaS management solutions. When will the NDcPP provide flexibility for certification for SaaS managed products?"

How is CC used now in government in the Cloud?

- Still a procurement checkmark item
- Some countries mandate CC, while others provide “guidance”

Cloud Usage of CC:

- US--CC Preferred for FedRamp, required for IL5 or higher
- Germany-- mandates EAL4 for BSI C5 (Germany’s reqs for ES Cloud)

- Question: But what is a CC evaluation in this context?
- Answer: It is an on-premises certificate not tested in a cloud environment.

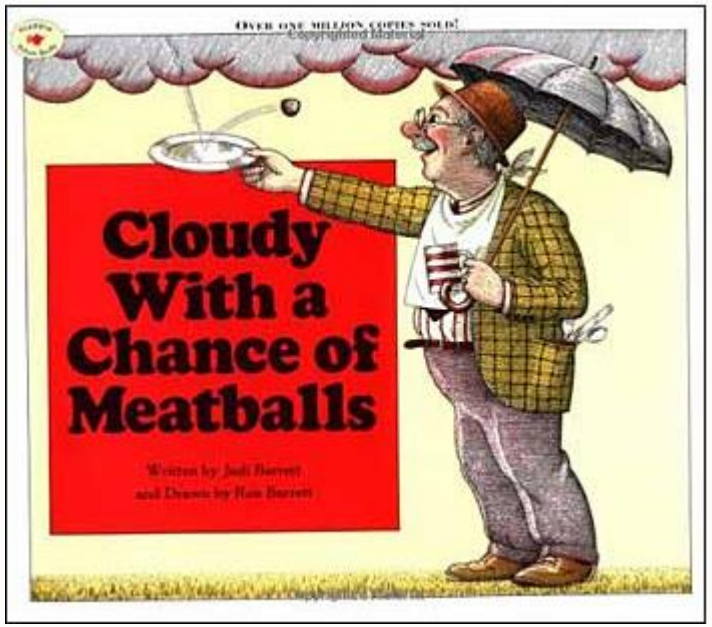
Children's Books and CC in the Cloud

- When I first presented this concept, I used the analogy of "The Emperor Has No Clothes" to express the theory that at some point someone would notice that CC has no value today for cloud deployments

https://cutewallpaper.org/download.php?file=/24/emperor-clipart/193991753.jpg (free use)

Cloudy with a chance of….

- Weather forecasts often use the phrase “Cloudy with a chance of rain”
- Continuing my theme of children’s books let’s look at “Cloudy with a Chance of Meatballs”



https://www.the-best-childrens-books.org/Cloudy-with-a-Chance-of-Meatballs.html

So why Cloudy with a Chance of Evaluating?

- As you have heard today, CC is a product evaluation scheme
- CC does not include nor allow for the evaluation of products in a dev ops environment.
- This project aims to change that notion

PPs, cPPs and iTCs

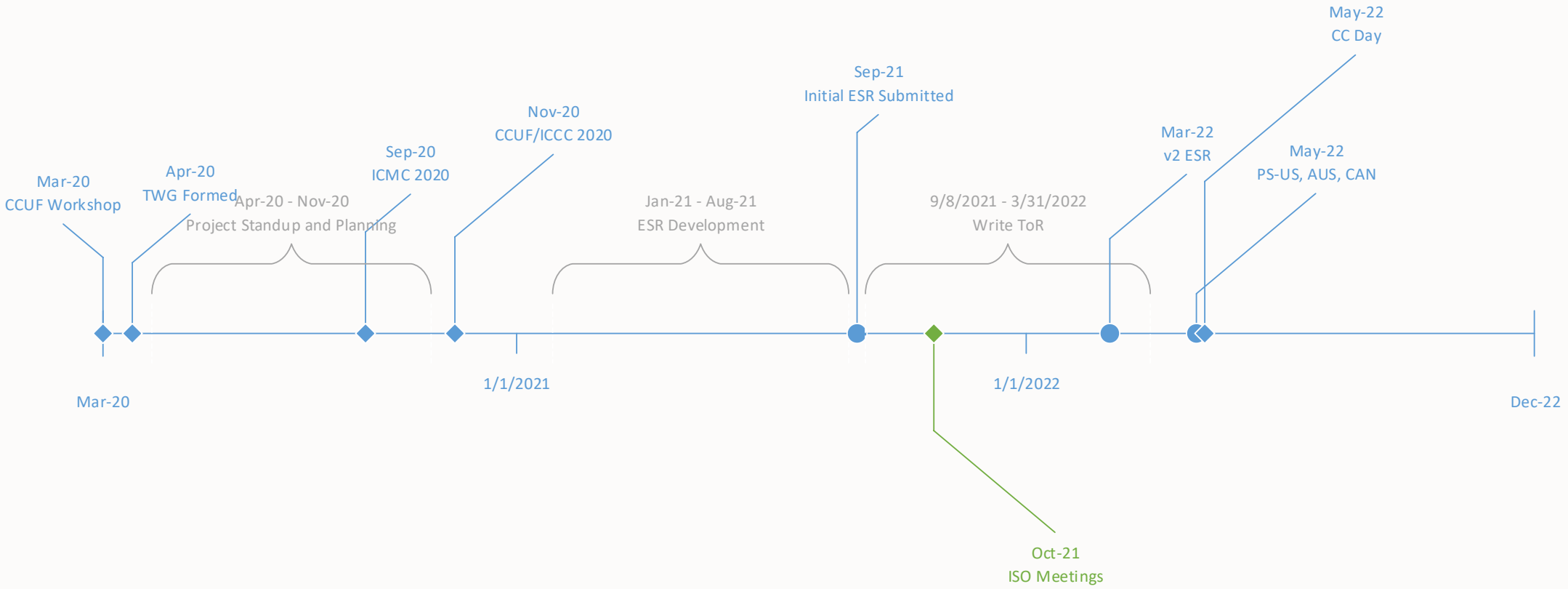
- **A quick primer on Protection Profiles etc.**
  - A Protection Profile (PP) is a set of security functions combined with specific testing approaches to provide assurance
  - A collaborative Protection Profile (cPP) is a PP that is built under the auspices of an international Technical Community (iTC)
  - Under the new CCRA ratified in 2014, cPPs are by default mutually recognized by all 31 countries in the CCRA
- **Why become an iTC?**
  - Only iTCs are authorized by the Common Criteria Development Board (CCDB) to write cPPs and their modules / supporting documents
  - Many hurdles to becoming an iTC with the first being an Essential Security Requirements (ESR) document being agreed upon by at least 2 countries in the CCRA

CC in the Cloud Technical Working Group (TWG)--Accomplishments

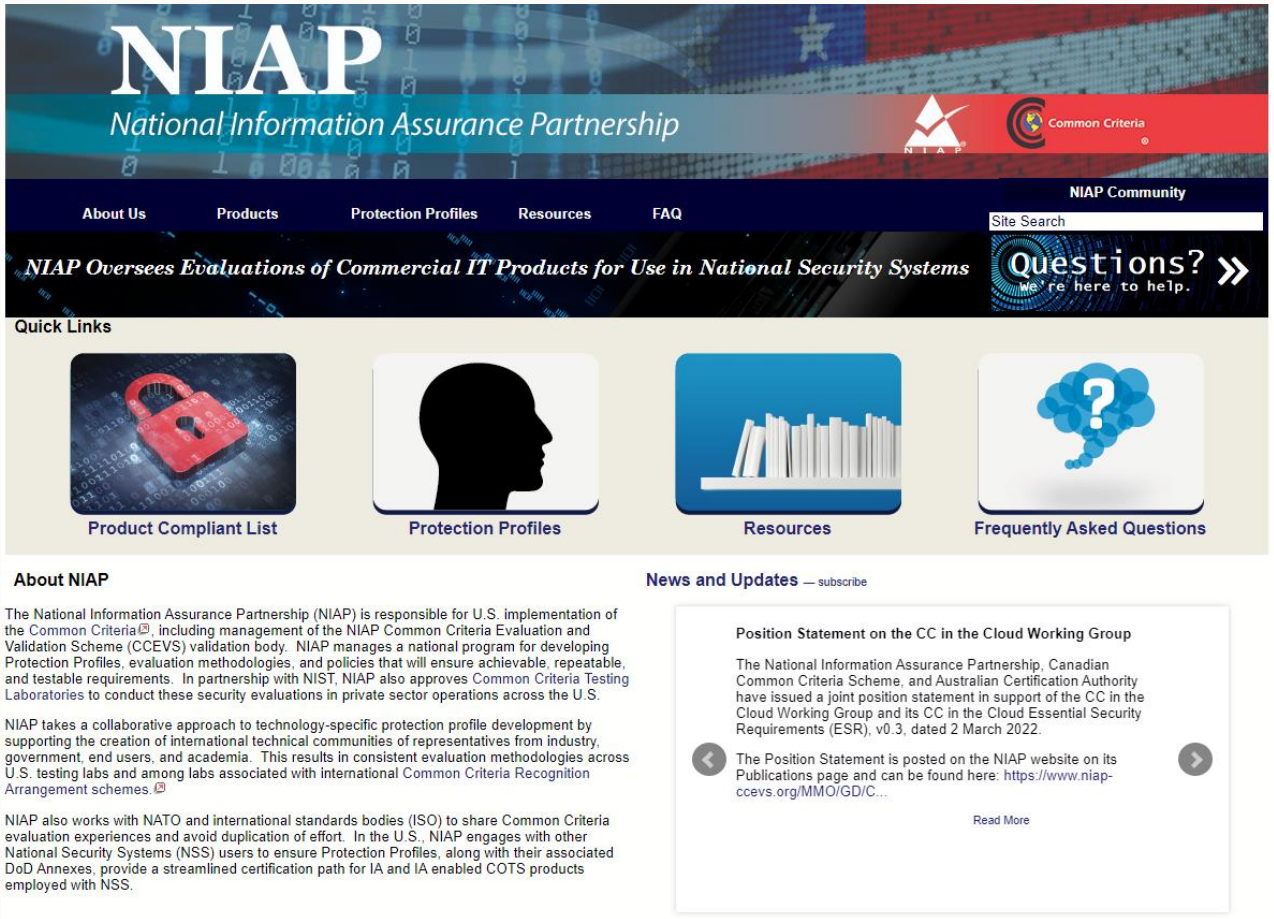
- ✓ Formed in March 2020 (Now up to 56 members)
- ✓ Created Problem Statement
- ✓ Determined SMART* Goals
- ✓ Published initial status report
- ✓ Launched Preliminary Work Item (PWI) with ISO
- ✓ Invited to present at ICMC, ICCC and CCUF
- ✓ Drafted ESR
  - ✓ NIAP and Canadian scheme feedback
  - ✓ 2nd Draft now with CCDB (approved by Canada, Australia and US)
- ✓ Completed other iTC requirements (Key Persons and Terms of Reference)

*Specific, Measurable, Achievable, Realistic and Timely

Timeline



Position Statement of US, Canada and Australia



Joint NIAP/CCCS/ACA Position Statement
CC in the Cloud Working Group
Essential Security Requirements Version 0.3, dated 2 March 2022

27 April 2022
Version 1.0

STATEMENT: The National Information Assurance Partnership (NIAP), Canada Common Criteria Scheme (CCCS), and Australian Certification Authority (ACA) agree with the content of the CC in the Cloud Essential Security Requirements (ESR), version 0.3, dated 2 March 2022.

PURPOSE: The intent of this Position Statement is to make it publicly known that NIAP, CCCS and ACA:

- recognize a need for evaluated products that are suitable for use cases identified in the ESR, and;
- agree that the ESR appropriately scopes the security challenges of such products.

SCOPE: NIAP, CCCS and ACA will revisit their positions as the CC in the Cloud Working Group develops its guidance.

If NIAP, CCCS and ACA endorse the resulting guidance, products evaluated against a Protection Profile which incorporate the guidance will be placed on the NIAP product compliant list (https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm), CCCS list of certified products (https://www.cyber.gc.ca/en/certified-products), and Common Criteria Portal certified products list (https://www.commoncriteriaportal.org/products).

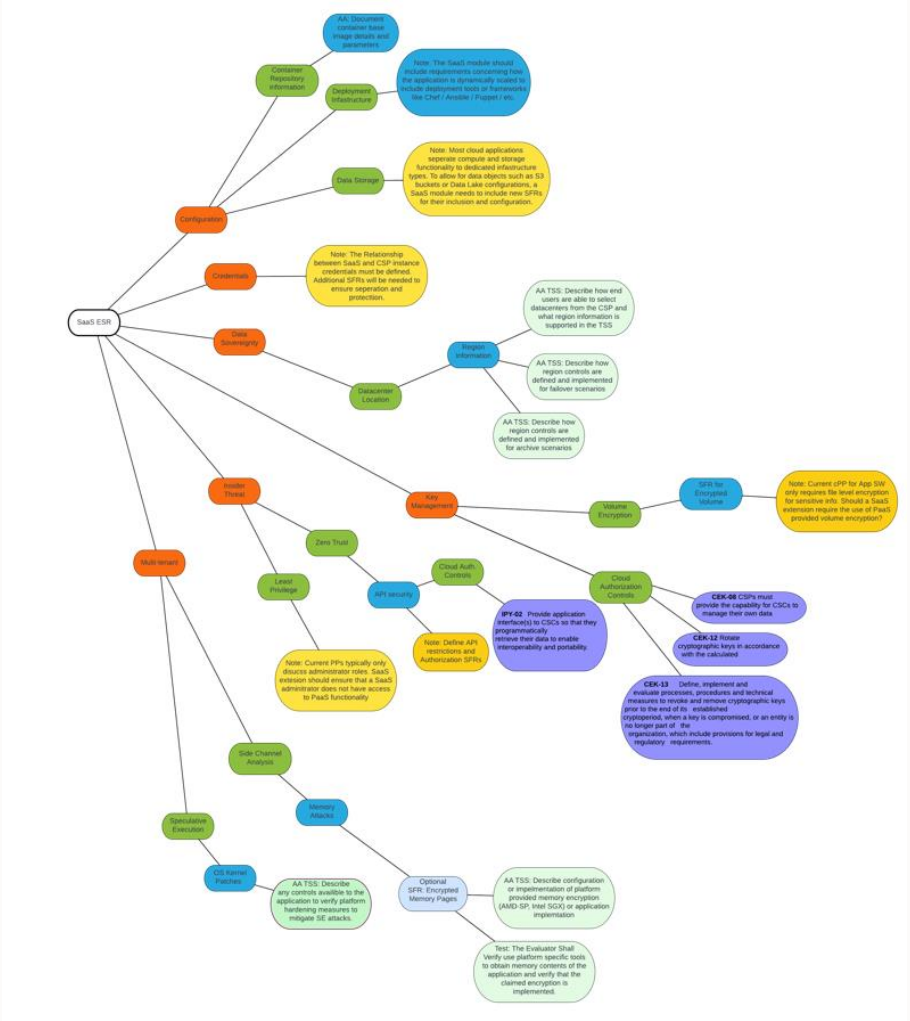
NIAP ACSC Australian Cyber Security Centre

https://www.niap-ccevs.org/MMO/GD/CC%20in%20the%20Cloud%20Position%20Statement%20v1.0.pdf

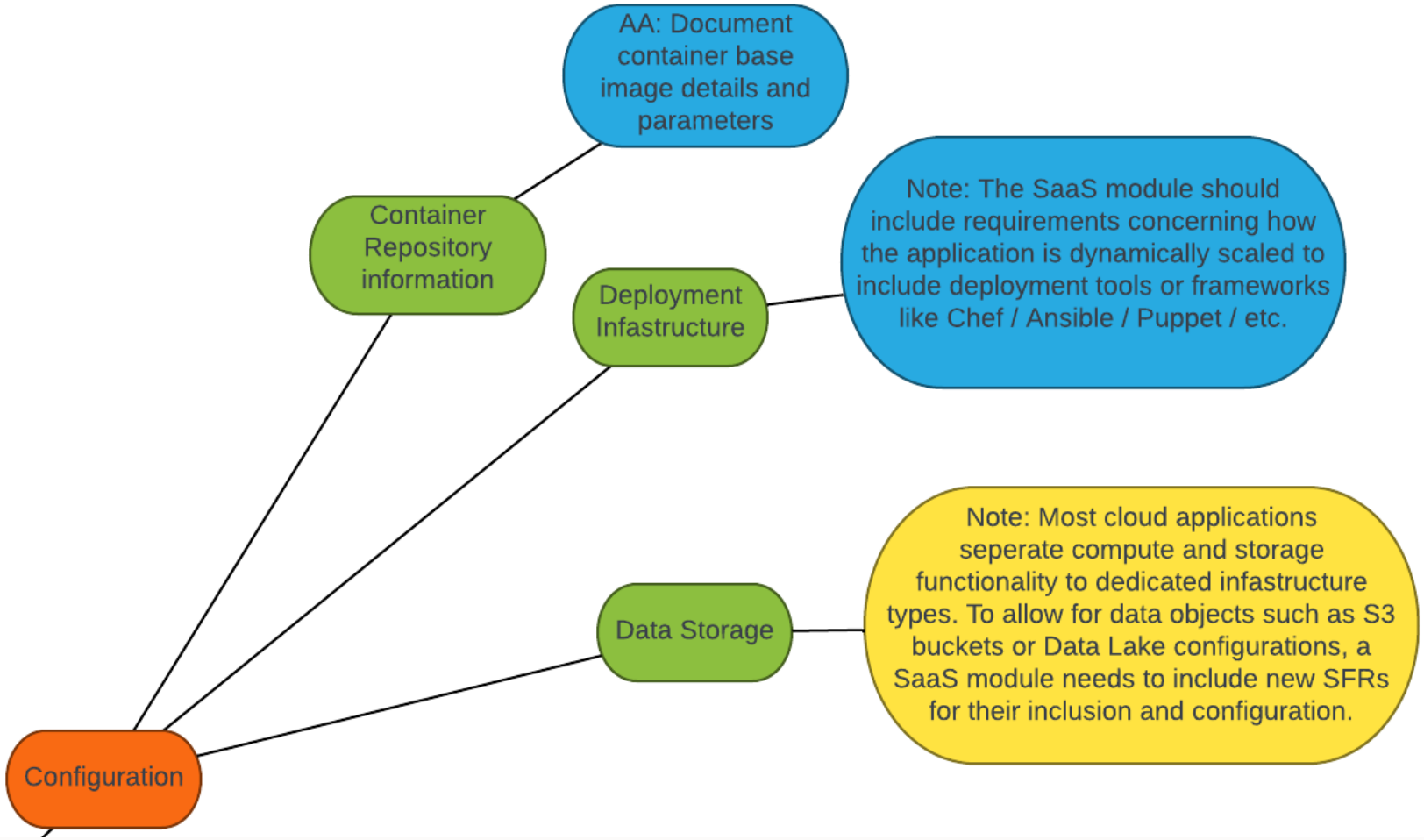
Essential Security Requirements (ESR)

- Utilizing GitHub
- Use Cases denoted by Protection Profile (PP)
  - Virtualization, OSPP, NDcPP DBMS etc.
- Known Evaluation Gaps
  - CC evals are Static
  - Use of Cryptography
  - Platform Abstraction
  - Environmental Evolution
- Threats
  - Configuration
  - Credentials
  - Data Sovereignty
  - Key Management
  - Insider Threats
  - Multi-tenant
- Assumptions
  - Trusted Platform
  - Trusted Provider/Admin
- https://github.com/CC-in-the-Cloud/Admin/blob/Working/ESR/CC%20in%20the%20Cloud_%20ESR.adoc

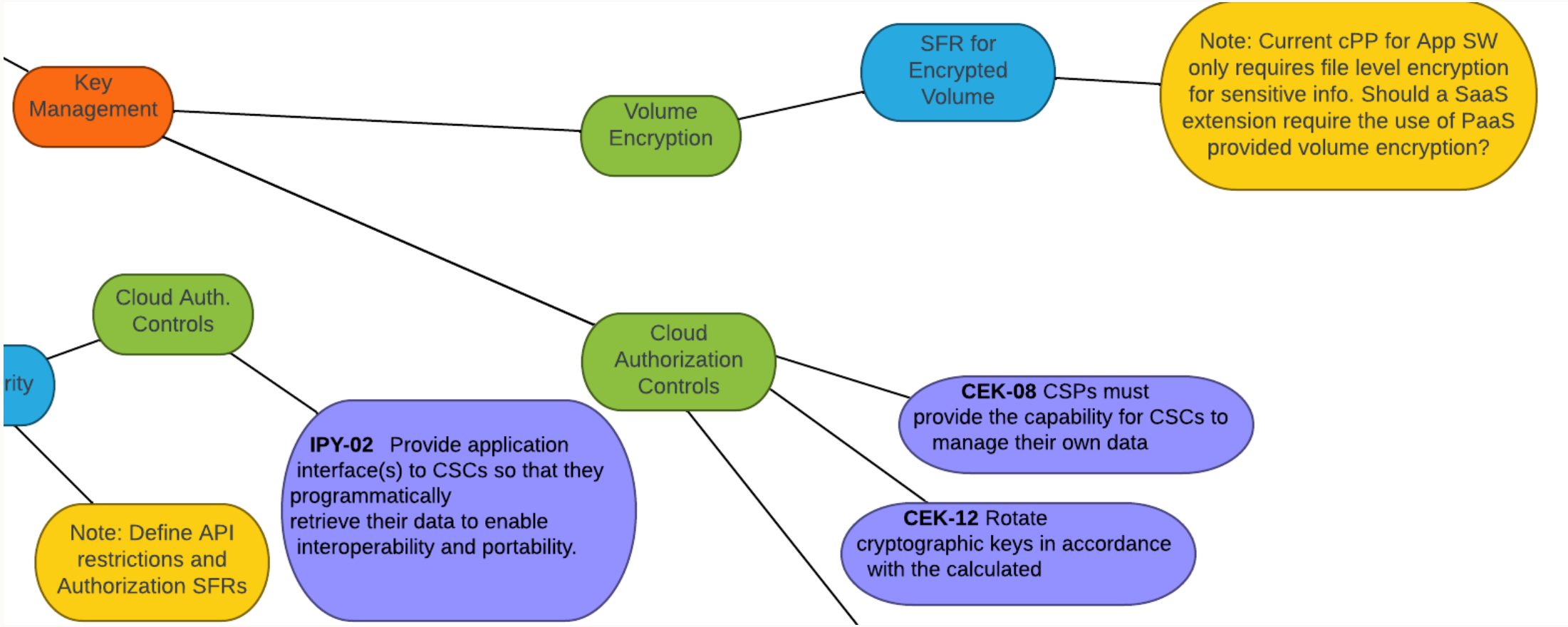
Building out CC in the Cloud Using MindMaps



Building out CC in the Cloud--Configuration



Building out CC in the Cloud—Key Management



Some Next Steps

1. Conference Presentations Continue: CC Day, CCUF, ICCC
2. Officially listed as an iTC
3. Trusted Platforms Sub-Group—to be created
4. Scheme/ Customer Requirements Sub-Group
5. Draft Guidance

Long term or Aspirational Goal-a Reminder

- CC for ICT products running in cloud (not CC for services or cloud providers)
- Providing assurance for products in a cloud scenario (not for the cloud administrative functionality—this is what the Trusted Provider part will cover)
- Have the CCRA formerly accept solutions to evaluate IT products in the cloud
- Provide guidance to evaluate a product/service in a cloud environment:
  - Short term via modules/supporting documents
  - ~5 years--Next version of Common Criteria ISO standard (15408)

Challenges

CC in the Cloud is HARD

- Does not fit CC today
- The current standard does not allow for service evaluations. We are focused on product evals in a devops deployment
- Equivalence?

Resources

- We have 56 members but really only about 10-15 are showing up to meetings
- Limited travel (so very slow progress virtually)
- Need consistent participation from vendors, labs, consultants

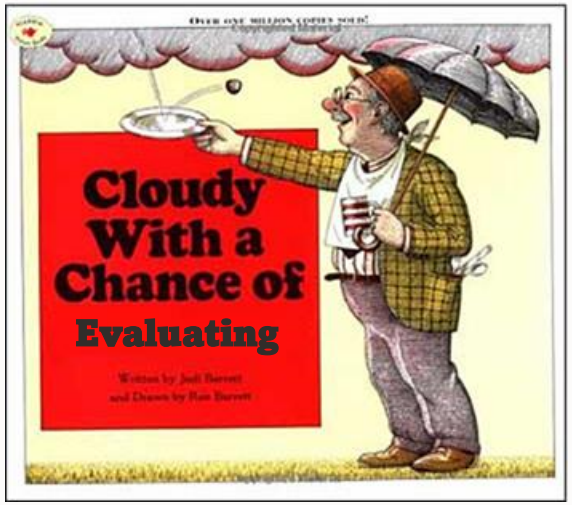
Industry Led

- NIAP took an active role in late 2021
- Industry led TWGs are harder for schemes to buy into
- Mostly schemes have been observers vs providing new ideas
- This TC will have an end user in leadership (vice chair from DISA)

Who we are:

- ***The team is comprised of 58 members including about 15 active members***

Questions?



Thank you!

Joshua Brickman

Joshua.Brickman@oracle.com

https://cc-in-the-cloud.github.io/ccinthecloud.github.io/

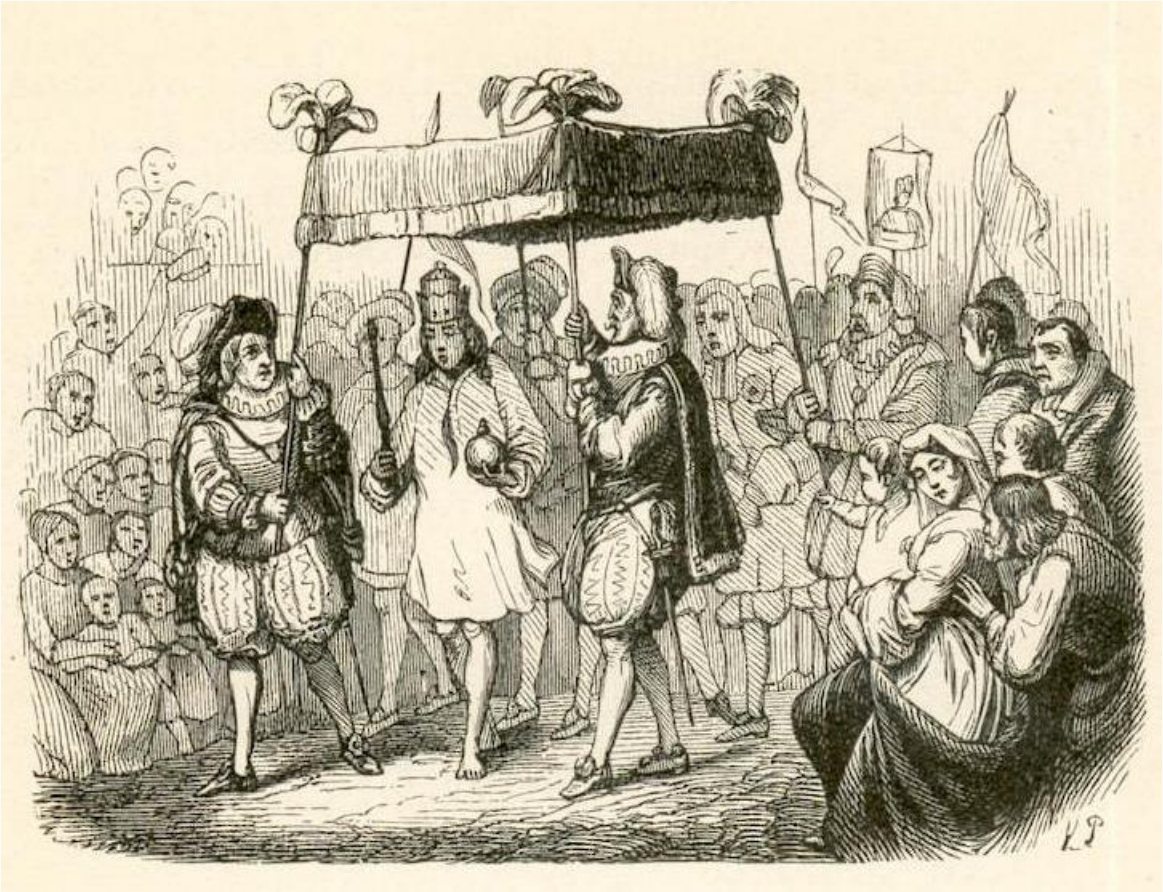
Initial Plan

- ✓ Draft a Problem Statement
- ✓ Establish SMART (Specific, Measurable, Achievable, Realistic, Timely) Goals
- ✓ Identify customers who are interested and other interested parties
  - Find any FedRamp contacts (still a to do)
  - Talk to EUCSA Cloud team (still a to do)
- ✓ Notify schemes of this project

SMART (Specific, Measurable, Achievable, Realistic, Timely) Goals

- ✓ Get ISO SC27 WG 3 to approve a new “Preliminary Work Item” on CC evaluations in the cloud
  - ✓ Assign sub team
  - ✓ Draft proposal
  - ✓ Circulate…
- ✓ Acquire informal approval of proposal with participating schemes within CCRA for output from TWG

The Emperor Has No Clothes!



- At some point customers are going to recognize that a CC evaluation of an ICT product provides little assurance in a cloud environment
- Without a plan for CC addressing, CC will become irrelevant in DevOps
- Customers will require additional country specific testing instead

https://en.wikipedia.org/wiki/The_Emperor%27s_New_Clothes#/media/File:Emperor_Clothes_01.jpg (free use)