The Internet Trust: Classic Scenario and IoT Scenario

SATO, Hiroyuki
The University of Tokyo
E-mail: schuko@satolab.itc.u-tokyo.ac.jp

@FutureComputing 2021, IARIA, April 18, 2021

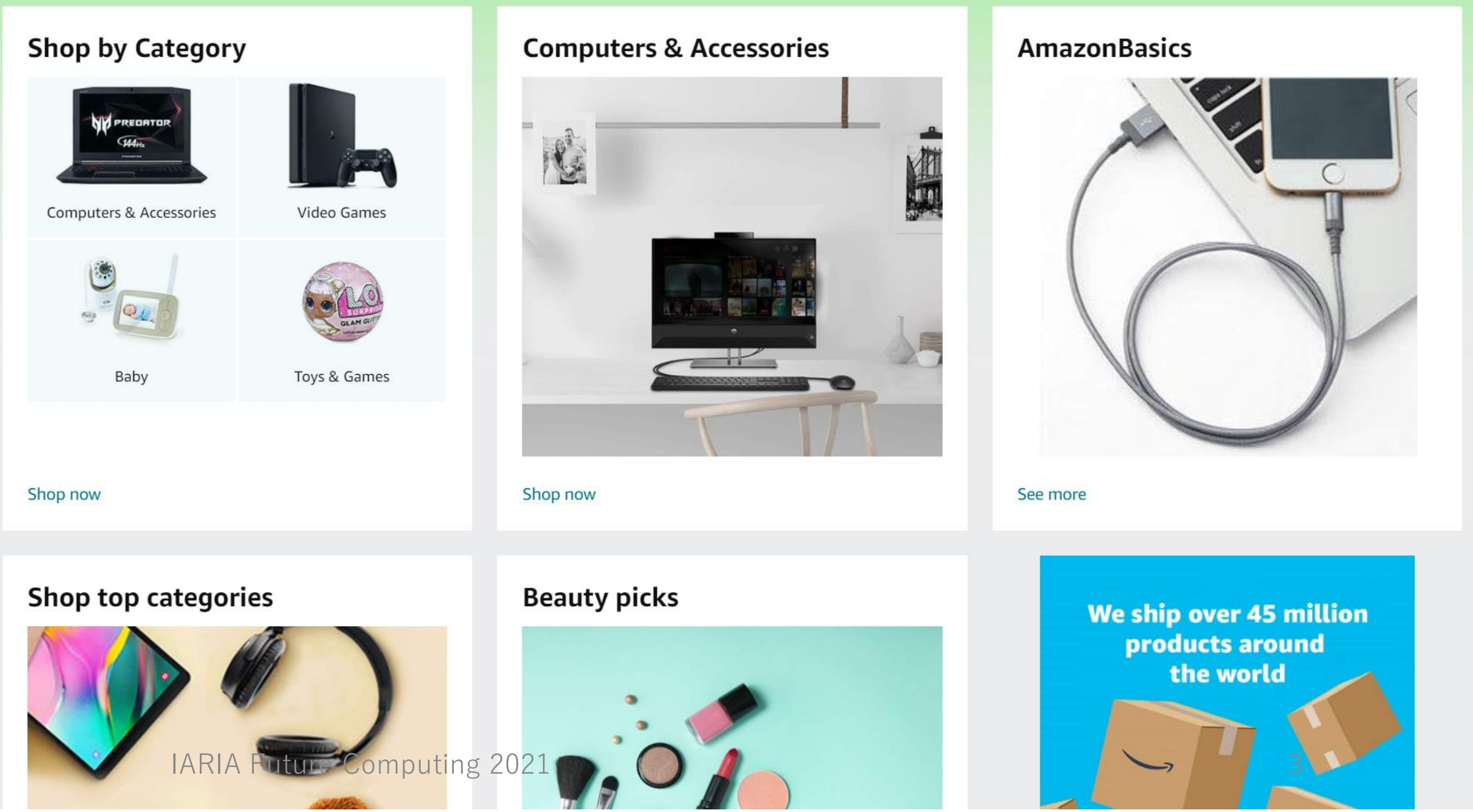
I am …

- Hiroyuki SATO, Dr.
    - Information Technology Center, the University of Tokyo, Japan.
    - Also involved in GakuNin, the Japanese Academid Access Federation Trust Framework.
    - Through GakuNin, Japanese universities collaborate with other academic access federations through eduGain.
    - GakuNin supports identity assurance level LoA 1 of Kantara. I serve Kantara as an LoA 1 assessor.
        - Federation and assurance are two keywords of this presentation.

Expanding Business in the Internet

- The Internet is spreading widely and deeply over every field of business.

From Amazon's Website →



Shop by Category

Shop now

Computers & Accessories

Shop now

AmazonBasics

See more

Shop top categories

Beauty picks

We ship over 45 million products around the world

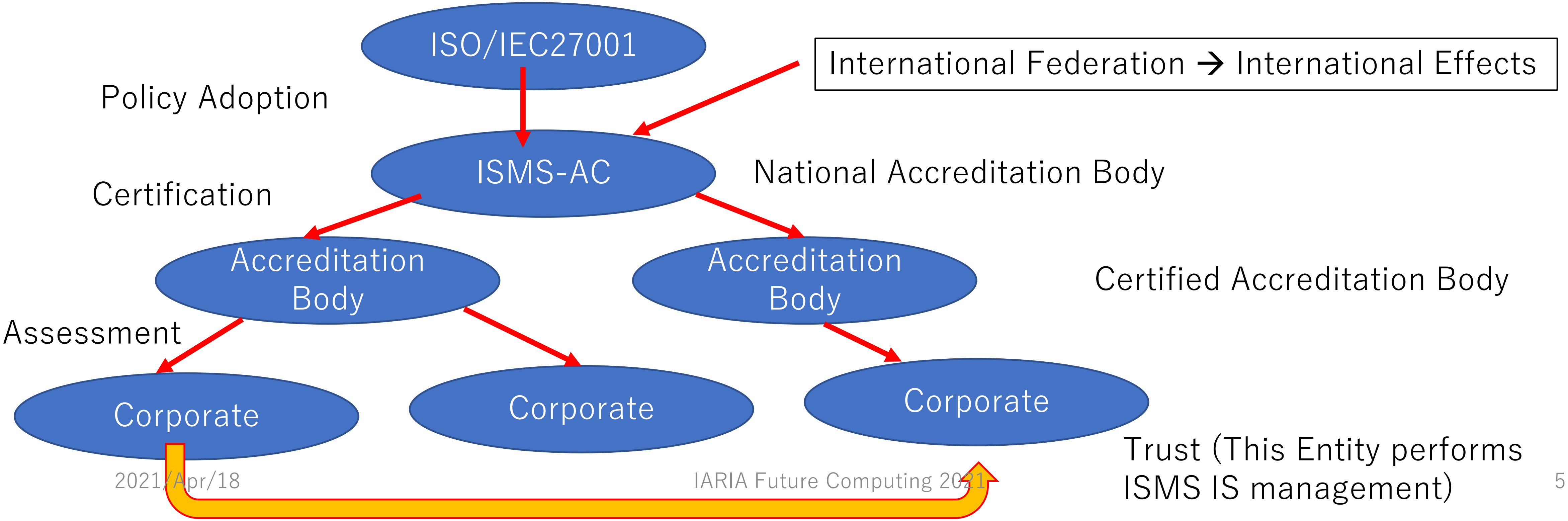
What is necessary in Business

- Trust relationship between entities
- Conventionally (non-Internet world),
  - Civil law
  - Contracts are protected under civil law(s)

- Typically, payment.
  - Bank system has been established to support indirect money exchange: bills
  - + Credit Card system for consumers
  - They work as a social infrastructure

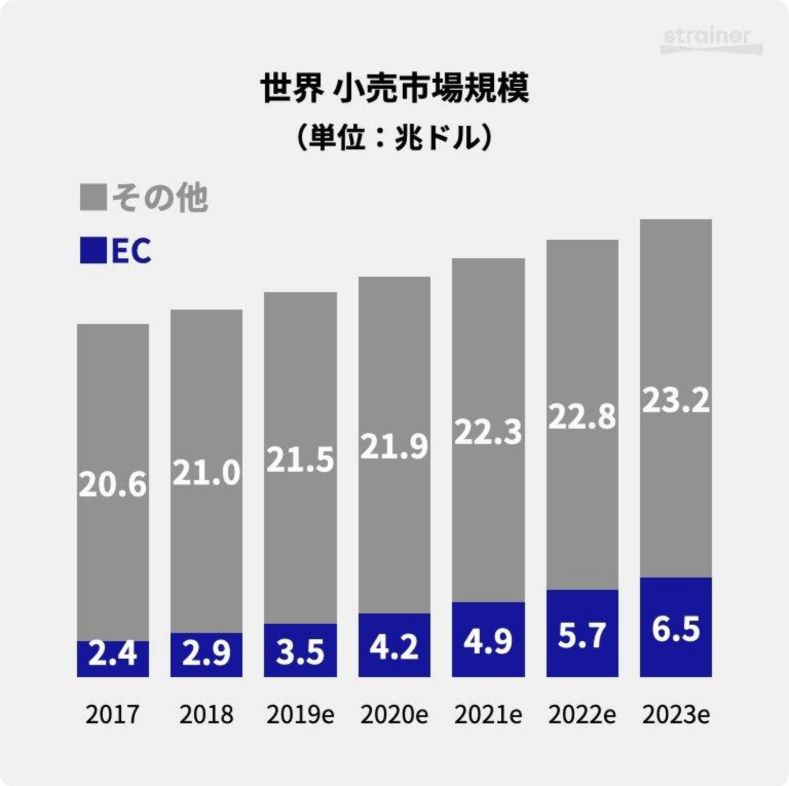
And Accreditation System

- Certification by Trusted Third Parties
  - Bank bill is trusted (anyway)
  - E.g. ISMS (Information Security Management System)


ISO/IEC27001
Policy Adoption
International Federation → International Effects
ISMS-AC
National Accreditation Body
Certification
Accreditation Body
Accreditation Body
Certified Accreditation Body
Assessment
Corporate
Corporate
Corporate
Trust (This Entity performs ISMS IS management)

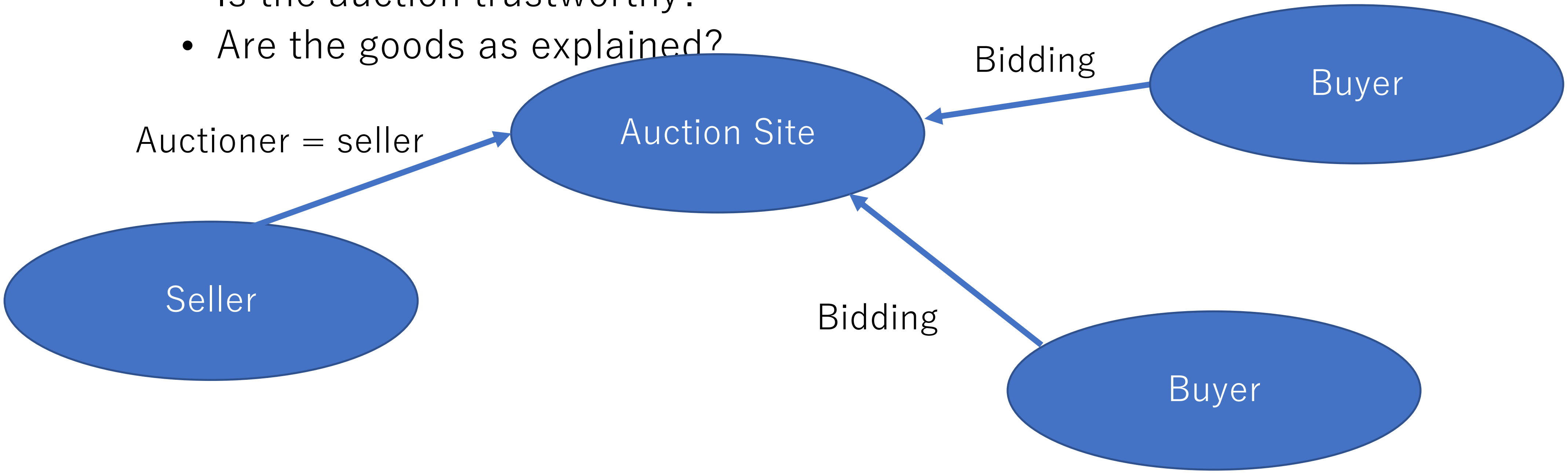
Different in the Internet world?

- Electronic Commerce
  - Payment Trust ← Most Important
  - This kind of Trust is supported by Technology: TLS and PKI
  - Rapidly Growing EC
    - Now China is the largest EC market.



Payment Trust alone?

- Consider Internet Auction Site
  - In Japan, the market is rapidly growing
  - However, we have a fundamental question:
    - Is the auction trustworthy?
    - Are the goods as explained?

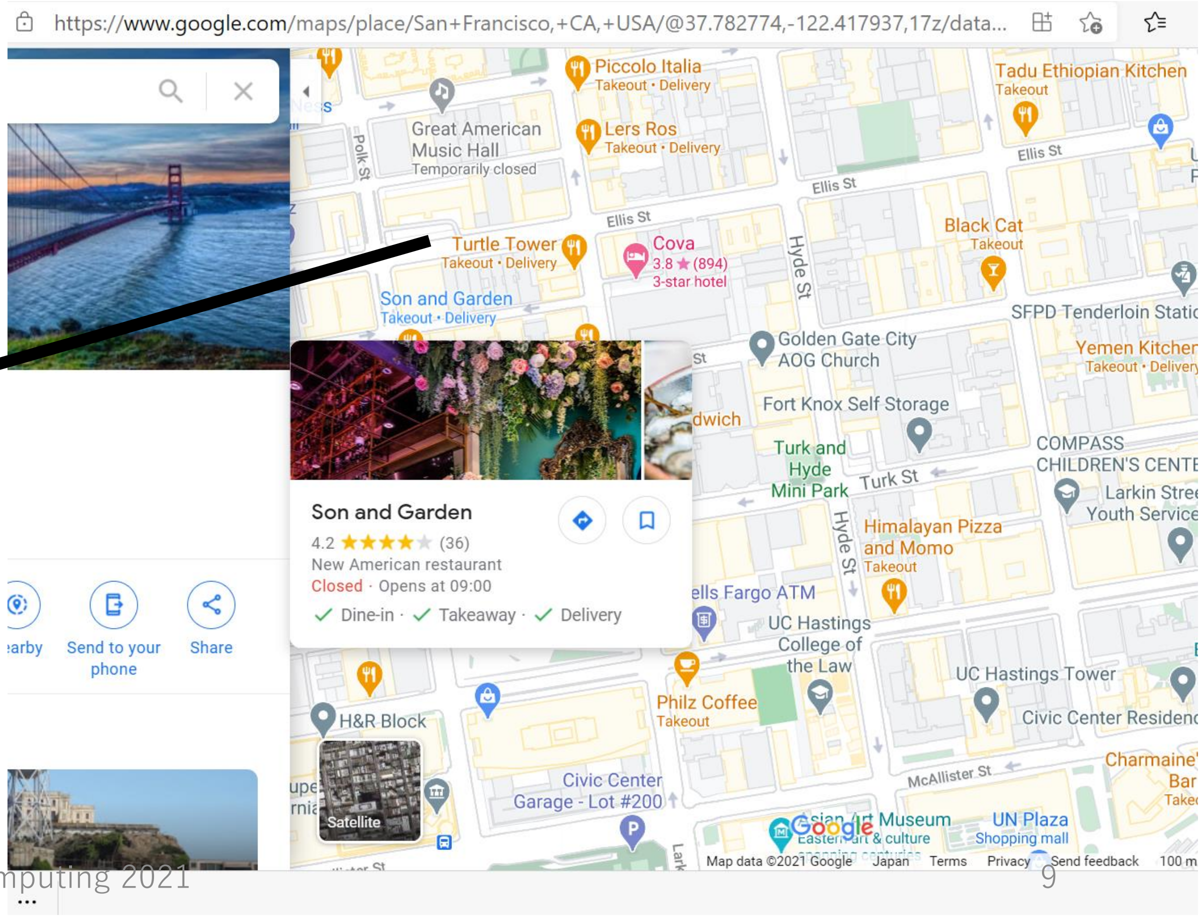


In this talk, we discuss Trust in the Internet

- In the Internet, we have a new form of services – Federated Service.
- In Federated Service, Trust is a fundamental component
  - So far, we have a number of experience scenarios.
  - For Federated Service, we have new technology support.
    - High assurance authentication
    - Sensitive Resourse
- The Internet Environment is fast changing
  - IoT, Edge Computing, decentralized computing, …
  - How to Establish Trust in such emerging envionments?

Classic Federation Scenarios

- The world is full of rich services:
  - For consumers’ world
    - For payment-required business, authentication is mandatory.

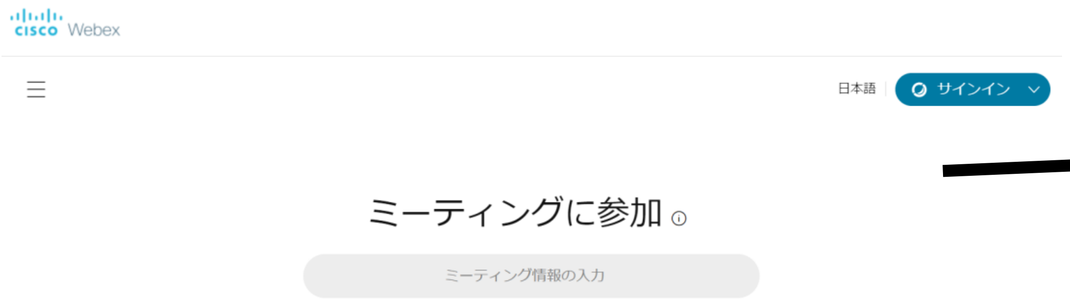


https://www.google.com/maps/place/San+Francisco,+CA,+USA/@37.782774,-122.417937,17z/data...

Son and Garden
4.2 ★★★★★ (36)
New American restaurant
Closed · Opens at 09:00
✓ Dine-in · ✓ Takeaway · ✓ Delivery

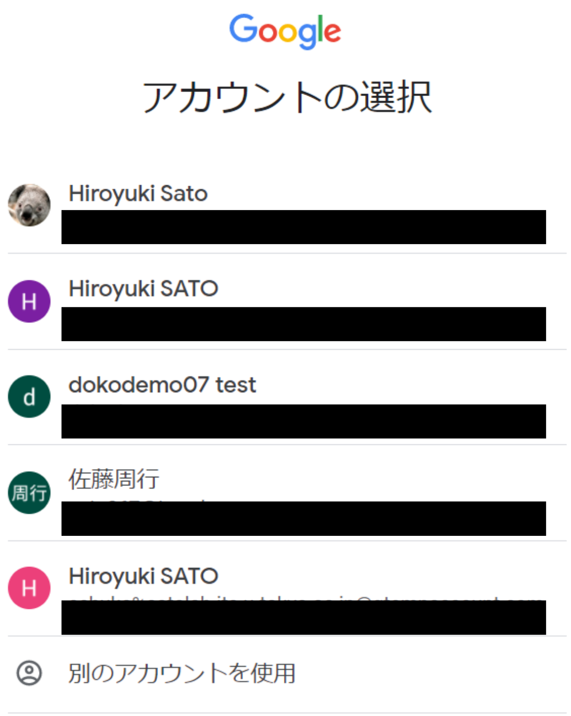
- For Consumer Services, accounts of Google, Facebook, etc. are used to form a federation.
    - Remember Account Chooser
- Many service providers trust the account information of Google or Facebook, and delegates the authentication to the IT giants.
- For Google or Facebook, this enlarges the opportunities (and values) of their account. → Win-Win in Federation.

- In Campus Life, we have common experiences of Federated Services.
  - Authenticate with Single Campus account
  - Use Campus Services with Single Account



ミーティングに参加

ミーティング情報の入力



Google

アカウントの選択

Hiroyuki Sato
[redacted]

Hiroyuki SATO
[redacted]

dokodemo07 test
[redacted]

佐藤周行
[redacted]

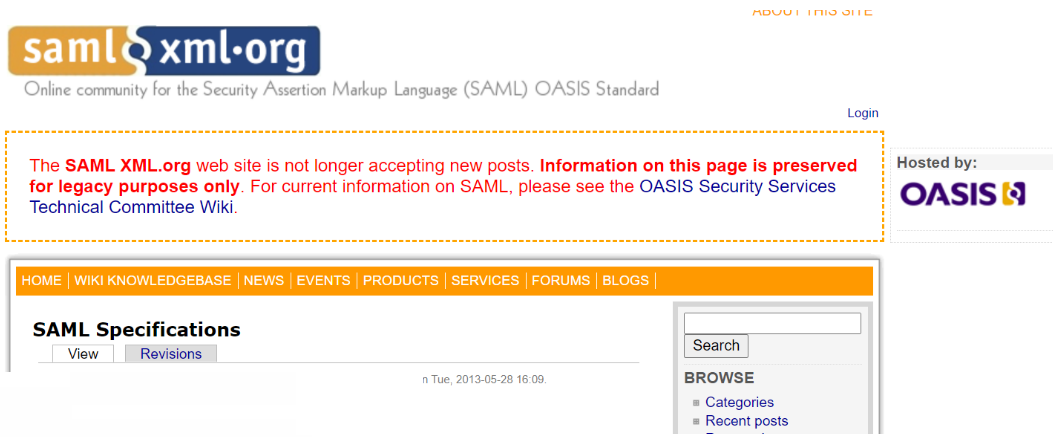
Hiroyuki SATO
[redacted]

別のアカウントを使用

- Actually, Identity Service is the most troublesome one.
    - Identity Life-cycle management
        - Registration Process, Update Process, Deletion Process,
            - For each step, we need Proofing or Evidence for Action.
    - Credential (Password) Management
        - Delivery, Update, Revoke
    - Authentication
        - Especially for Remote Authentication
- Other Services CAN trust the assertion of Identity Service Provider → It CAN use the assertion as Authentication
    - Advantages of Google and Facebook

Protocols for Service Federation

- Basic Protocol for federation.
  - Most common sequence assumes Web Browser’s functions
- SAML
  - XML based
- OpenID Connect
  - Json based
- OAuth2
  - authorization


saml xml·org
Online community for the Security Assertion Markup Language (SAML) OASIS Standard
Login

The **SAML XML.org** web site is not longer accepting new posts. **Information on this page is preserved for legacy purposes only**. For current information on SAML, please see the OASIS Security Services Technical Committee Wiki.

Hosted by:
OASIS
HOME | WIKI KNOWLEDGEBASE | NEWS | EVENTS | PRODUCTS | SERVICES | FORUMS | BLOGS |

SAML Specifications

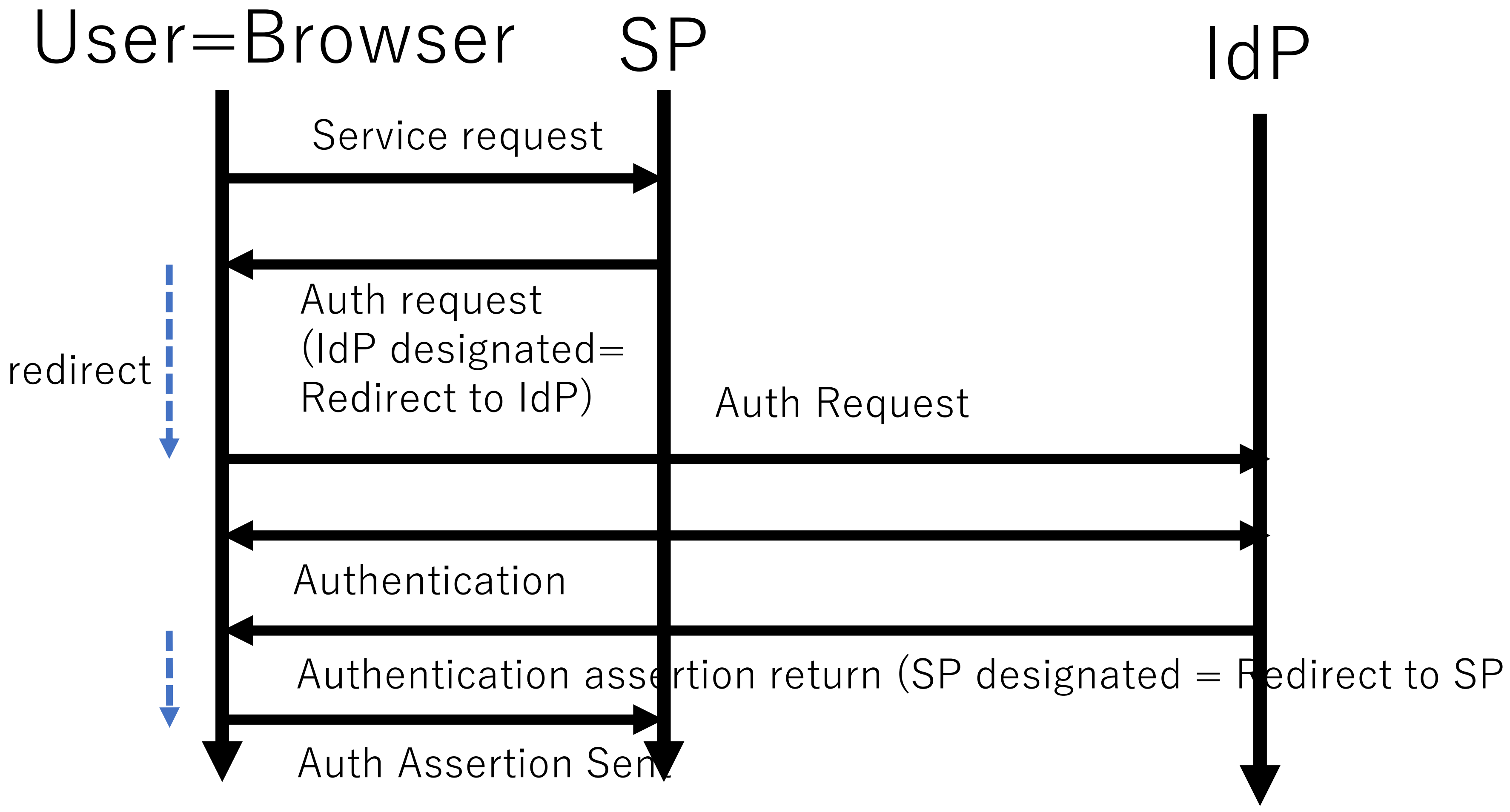
View
Revisions
n Tue, 2013-05-28 16:09
Search
BROWSE
Categories
Recent posts

Software

- Shibboleth (SAML IdP and SP)
  - For enterprise software

- Commercial Implementation (SAML, OIDC, OAuth2)
  - Google
  - Microsoft
  - Facebook
  - …

Typical Sequence – supported by browser



- Depending on
    - XML technologies – esp. XML signature
    - JavaScript technologies – esp. JSON signature

- Signature is used to keep the sequence consistent

- Browser technologies
    - HTTP redirect
    - Javascript

Conclusion 1

- Identity Service is THE key service in Service Federation.

- Then, How do we TRUST the Identity Assertion?

US Initiative

- OMB M04-04 (2003) E-Authentication Guidance for Federal Agencies
- NIST SP800-63 v.1 (2004) Digital Identity Guidelines
  - First Document that Defined the Criteria of Identity Assurance
    - Identity Proofing
    - Credential management and Authentication
    - Remote Authentication
  - First Document that Defined the Levels of Assurance
    - Levels 1—4.
- NIST SP800-63 v.3 (2017)[1]
  - RE-create SP800-63
    - Discuss each Criteria in separate documents
      - Identity Assurance Levels (IAL) 1--3
      - Authentication Assurance Levels (AAL) 1--3
      - Federation Assurance Levels (FAL) 1--3

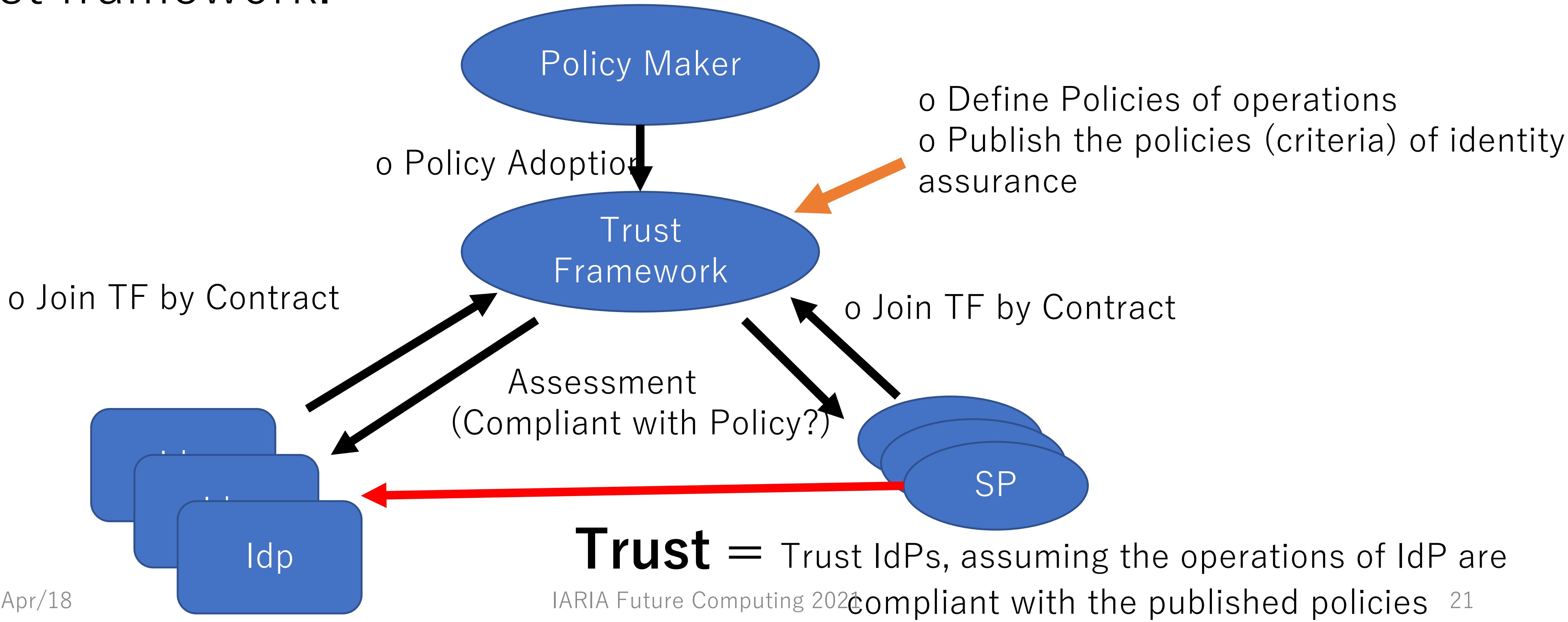
- Level of Assurance
- Assuming an Organization, Organizational account has some levels of identity assurance.
- Identity Proofing
  - Level 1 basically allows self assertion
  - Level 2 assertions are verified, anyway
  - Level 3 assertions are strictly attested and verified
- Authentication
  - Level 1 basically allows password
  - Level 2 combination of two factor authentication methods
  - Level 3 combination of two factor strict authentication methods

Control of SP?

- IdPs can be controlled by LoA
- SPs should be controlled by some criteria.
  - Like AUP in ISP.
  - There have been proposed a few criteria
    - Data Protection Enforcement (like PCI DSS)
    - Privacy Protection Enforcement (Regulataion)
    - Code of Conduct, or Ethical Regulation
  - No standard regulations, but something is assumed.

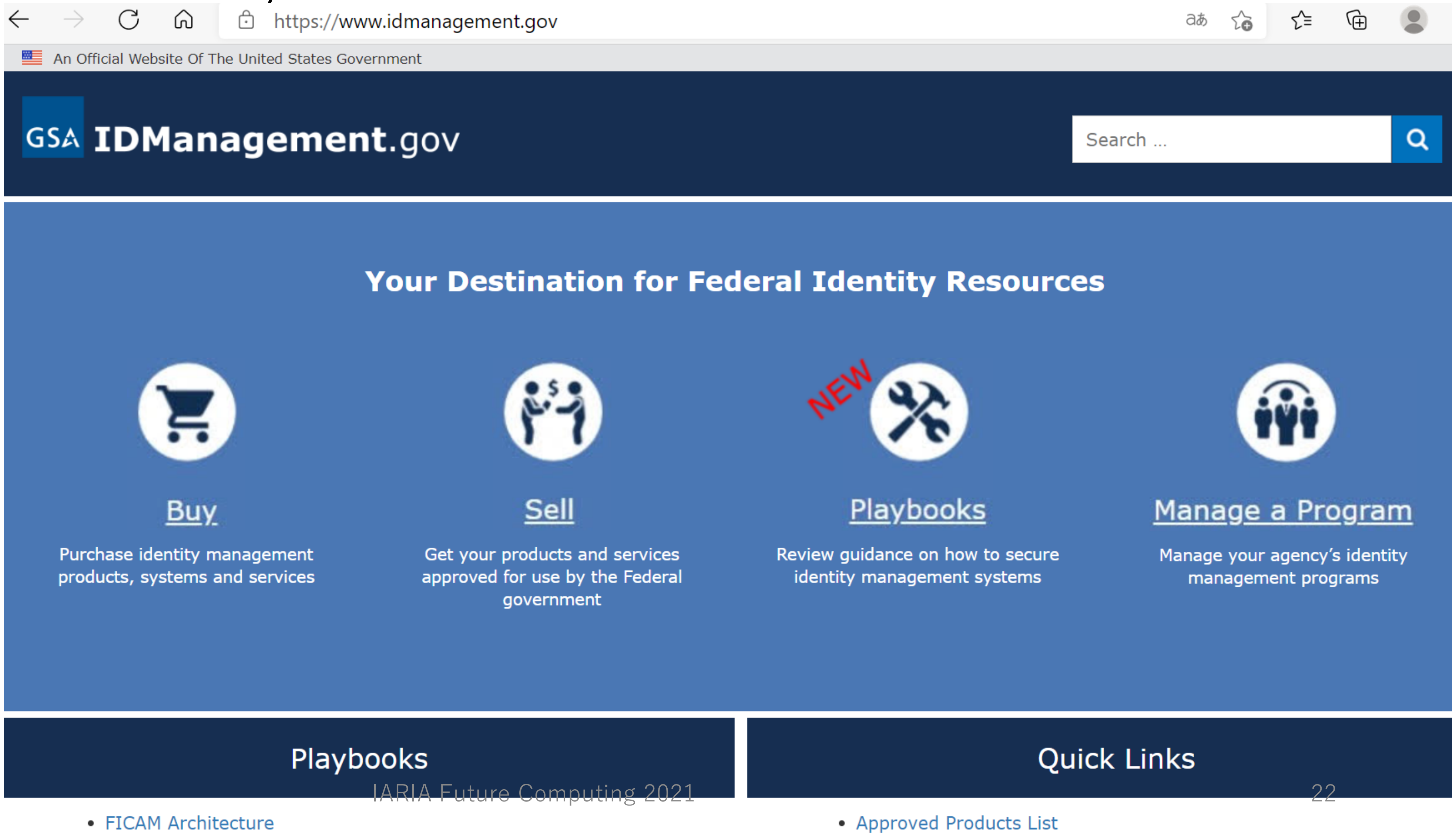
Operation Bodies = Trust Framework

- In Early 2010s, the idea of service federation has evolved to trust framework.



Trust = Trust IdPs, assuming the operations of IdP are compliant with the published policies

US Case Study



https://www.idmanagement.gov

An Official Website Of The United States Government

GSA IDManagement.gov

Search ...

Your Destination for Federal Identity Resources

NEW

Buy

Purchase identity management products, systems and services

Sell

Get your products and services approved for use by the Federal government

Playbooks

Review guidance on how to secure identity management systems

Manage a Program

Manage your agency's identity management programs

Playbooks

- FICAM Architecture

Quick Links

- Approved Products List

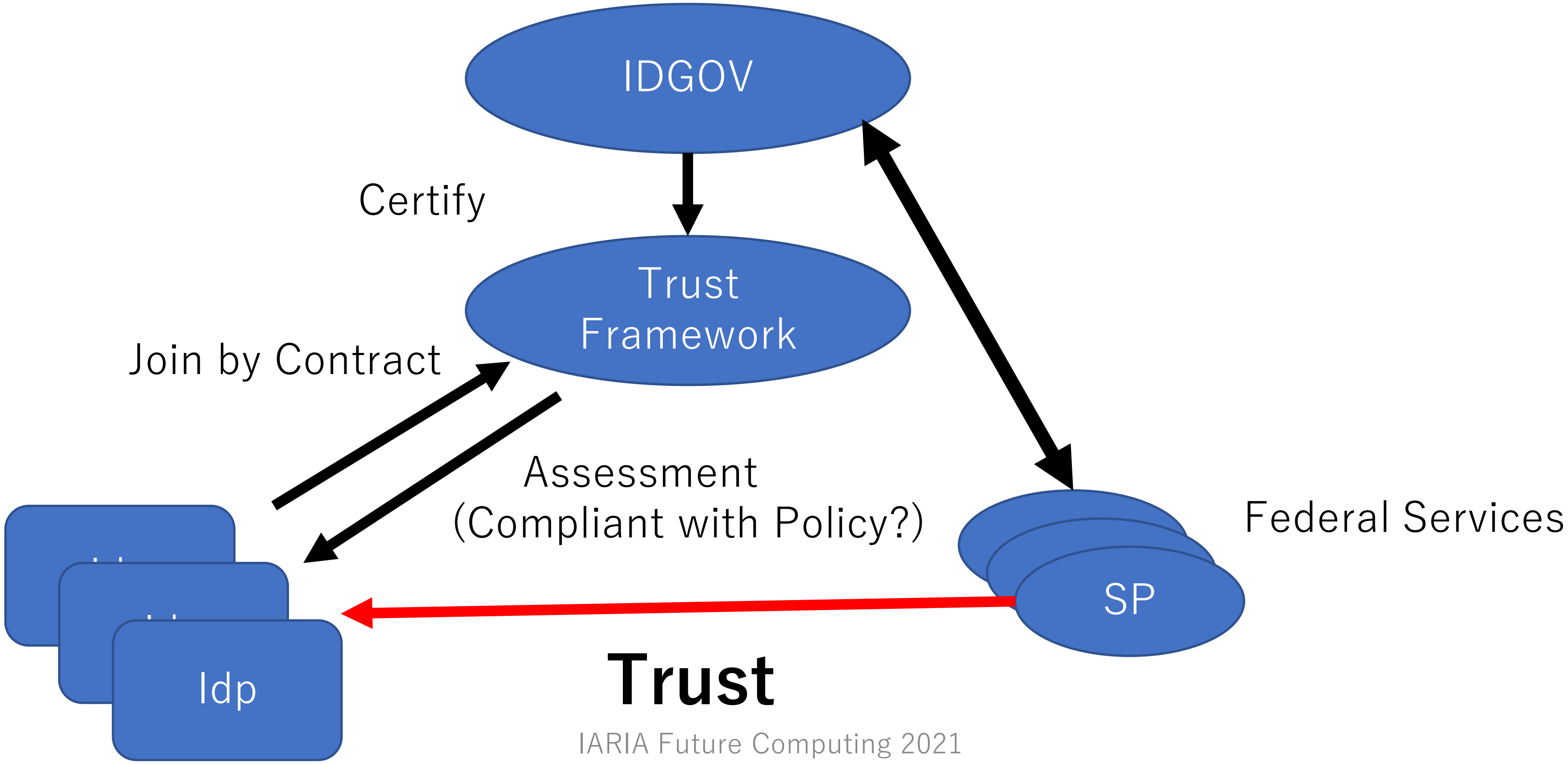
NSTIC

- National Strategy for Trust Identities in Cyberspace
  - 2011–
  - Leverage Identities of Private Sectors to use wide-range of Services including Federal Services

  - Government’s movement has changed to negative since 2016, but
  - Use of Identities of Private Sectors (Google, Facebook, Twitter, …) has become common!
  - Standard Protocols for Federations (SAML, OIDC) are used.

FICAM

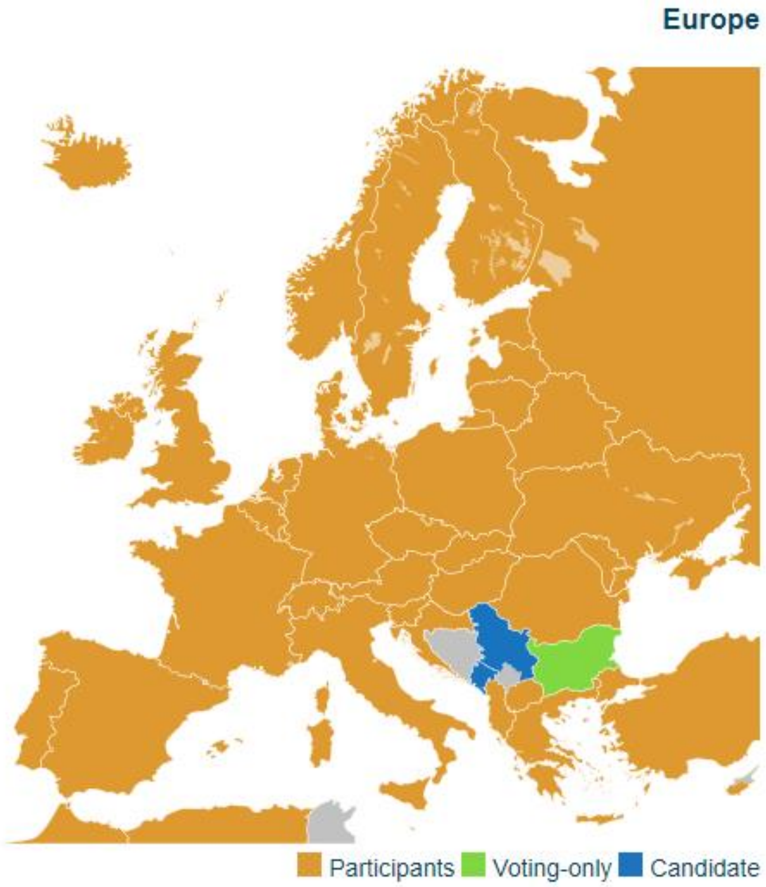
- Federal Identity, Credential, and Access management

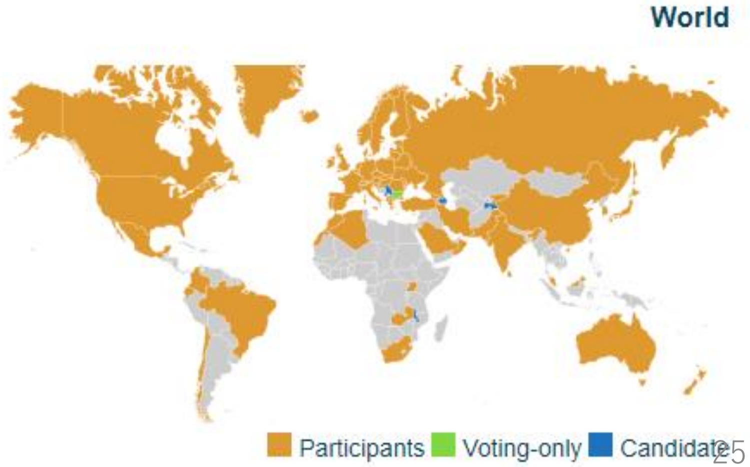


In Academia,

- In 2010s, nation-wide academic federations have been established
  - Original motivation: e-journals
  - US – InCommon
  - Japan – GakuNin

  - World-wide eduGain



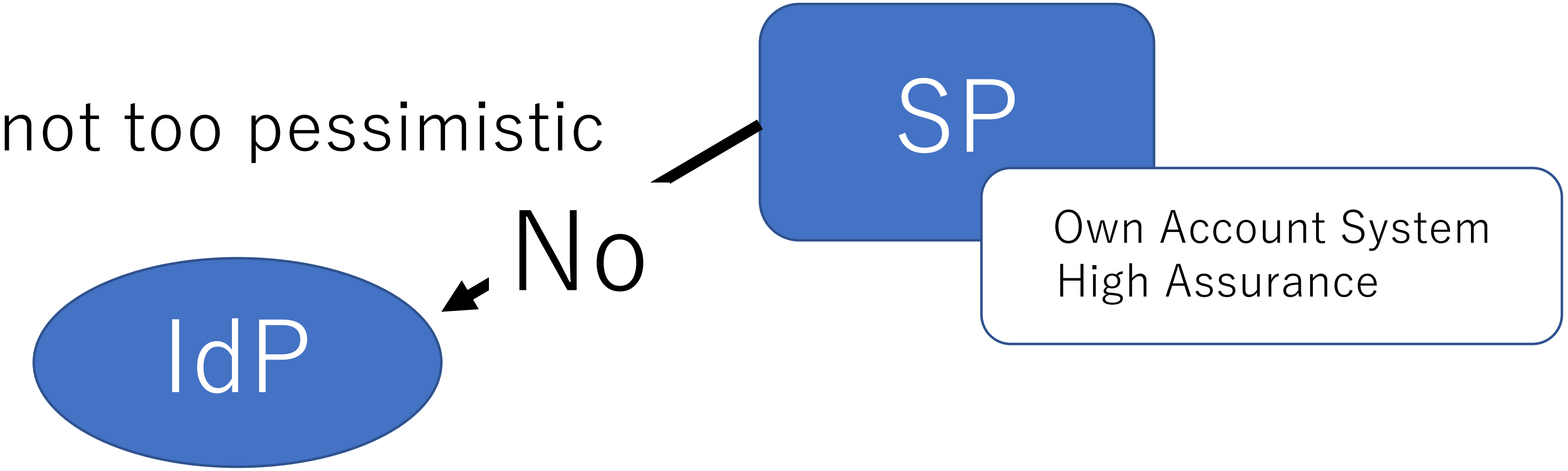


- Actually, Federations are Commonly used in our daily life.
  - Campus Services with SINGLE university account
  - Consumer Services with Consumer account

  - → Google or Microsoft may be a single service provider for those accounts

  - Inter-university Services with university account
    - Federated Service (nationwide academic federations or eduGain)
- **However, is it enough for handling sensitive data?**

- Bad Scenario:
  - Service Provider (SP) CANNOT trust the assertion of the Identity Provider
  - → SP must manage Authentication by itself
  - → SP must build its own Account System
  - → Extra Cost
- This scenario is not too pessimistic



- Healthcare
- University Finance
- University IR
- Data for Nobel-prize level research
- Precious Computing Resource
- …

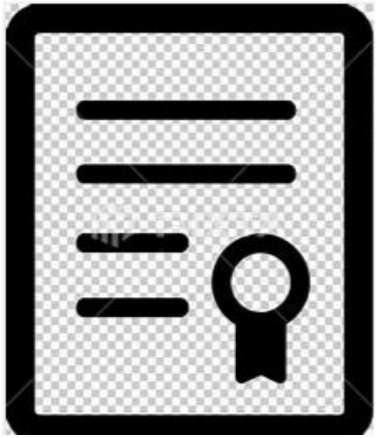
This means

- Critical and/or Sensitive Data/Resource → Joining Trust Framework as a Service Provider
  - Very nice, but it enforces HIGH LEVEL identity assurance.

  - Of course, a number of services that requires only “casual” identity assurance → Divergence of services

- Good News: Strict Authentication becomes common.

Hardware Solution



Software Solution

OOB Solution

- If appropriately operated, combination of these factors improves authentication assurance.
  - Two-factor authentication among
    - Knowledge (password) – Something you know
    - Possession – Something you have
    - Biometric – Something you are
    - (Behavior – Something you behave)
  - Risk analysis of two-factor authentication – NIST SP800-63 AAL
- + Risk based Authentication
  - Sophisticated Authentication with reasonable cost

Stratified Trust Framework

- Trust Overlay on a base Trust Framework
    - Participation of Casual Services Providers
    - Participation of Critical Services Providers

    - Users show casual/strict authentication assertion to those providers
        - In some case, password authentication, → casual services
        - In some case, additional certificate authentication → critical services

- In 2010’s, this scenario was considered to be hard to deploy.
- Now, it’s time to go ahead!

Japan’s approach – New Trust

- Japan, like Europe and US, has a number of projects that require high assurance authentication
  - Supercomputing services
  - Data platform services
- GakuNin, the Japanese academic federation, has decided to solve this problem by
  - Deploying High Assurance Identity Assurance in Universities
  - Calling for Assurance Requirements by Projects, and Reconciliate
  - Collaboration with Private Sectors
  - International Collaboration

New Trust

- GakuNin will Cover Japan’s Academic Identities
  - With Stronger Authentication methods
- For Accelerating Open and Secure Data Exchange, and
- Enabling High Level Research Collaboration in the Internet.

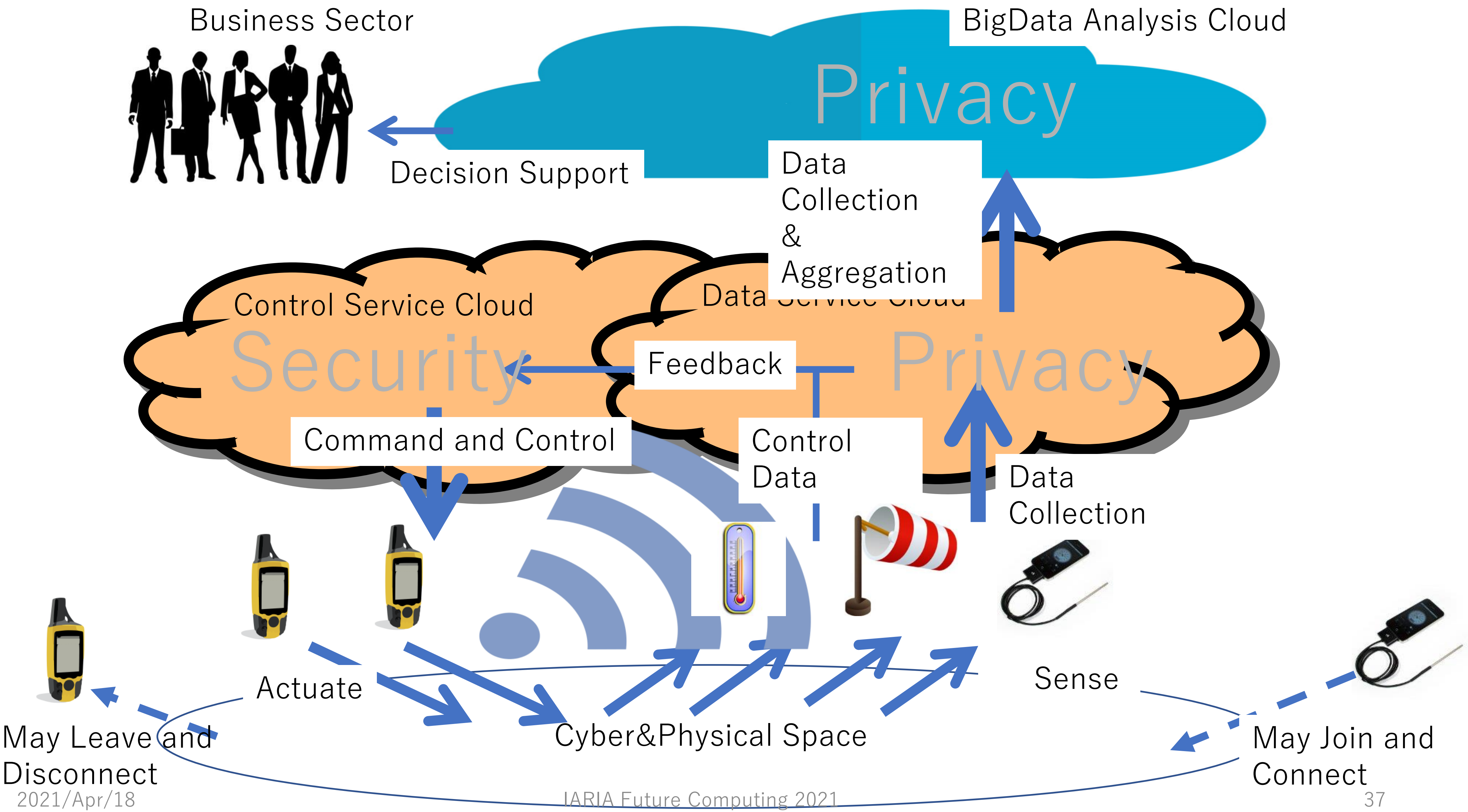
Another Movement

- Change of the Internet
  - Ancient: Nodes are Big Irons

  - Now: Light Mobile Clients access the Resource

  - Now and Future: IoT, the Network of sensors and actuators

- Management of the Network
  - We often cannot assume Well tailored Organizational Control anymore
  - Instead, Decentralized Movement
    - Blockchain, P2P, …
  - Instead, collection of local network
    - network of poorly powerful sensors
  - They dynamically join and leave the network.
  - Conventional static model of Data Trust does not apply



Business Sector

BigData Analysis Cloud

Privacy

Decision Support

Data Collection & Aggregation

Control Service Cloud

Security

Data Service Cloud

Feedback

Privacy

Command and Control

Control Data

Data Collection

Actuate

Sense

Cyber&Physical Space

May Leave and Disconnect

May Join and Connect

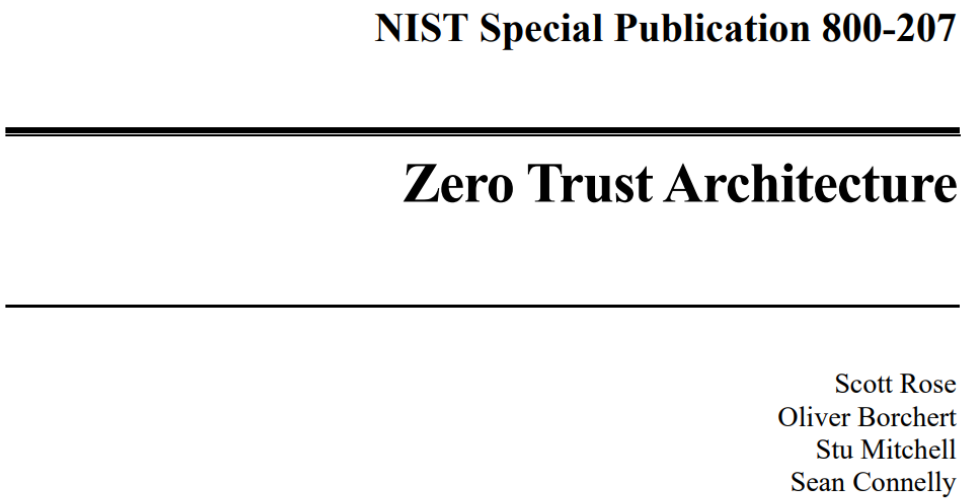
Typically

- What are Identities in the dynamic network?
  - The data owner may have left the environment.
  - Newly joining entities have no trust at the moment of joining.
  - Leave/Join is not based on any contract. They suddenly appear, and suddenly disappear.

- The entities may be malicious (They join and connect without any contract.)

- What kind of Trust must be there?

- Zero Trust has been proposed [2].
  - Authentication is Mandatory at every (micro)-Step
  - Policy is dynamically determined



NIST Special Publication 800-207

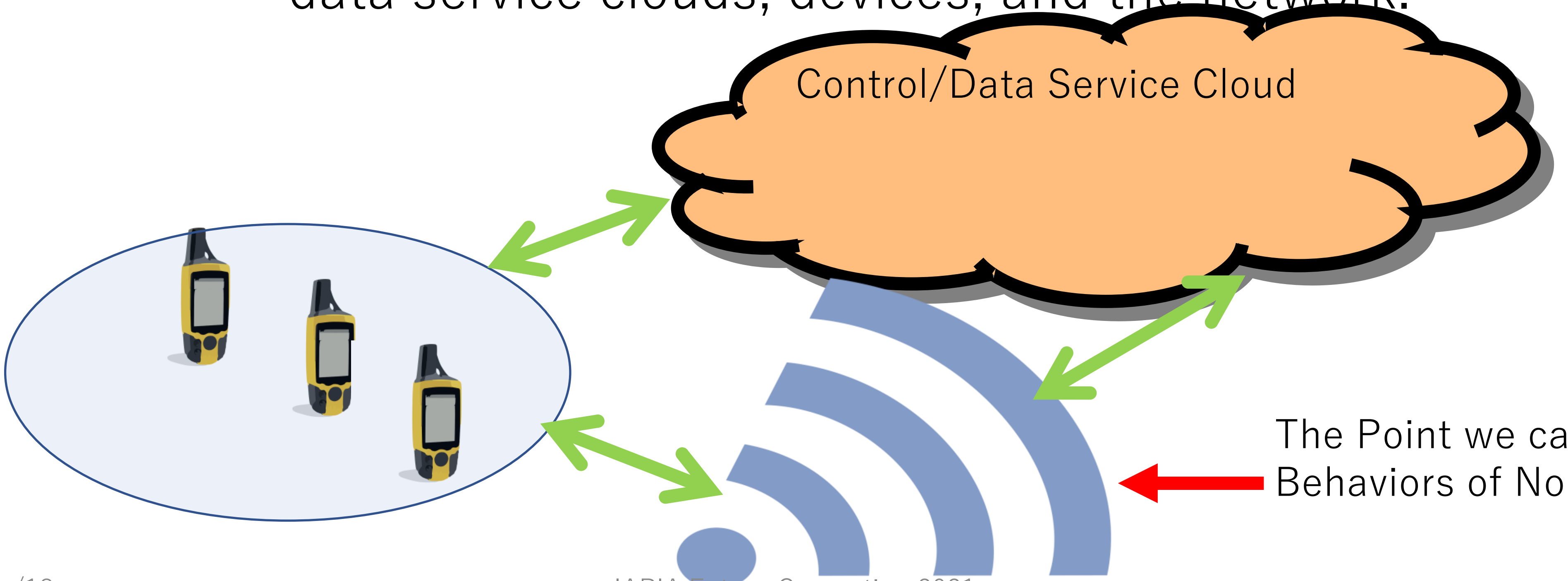
Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

- However, in IoT, such architecture does not apply.
- Solution 1. Specify Area where trustworthy behaviors are observed [3].
    - Specify Connection Criteria
        - Device Identification
            - Can we identify all devices?
                - Yes, if the number of devices is small.
                - No, if large in volume, or if they are mobile.
        - Connection process to devices
            - Can we authenticate the connection?
                - NO: NFC
                - Yes: BT (strict operation), WIFI
        - Connection protocols
            - Key generation and pairing processes
                - Simple but weak, or
                - Complicated but strict

Area Trust

- Area is
  - Spatial extent that accommodate control and data service clouds, devices, and the network.



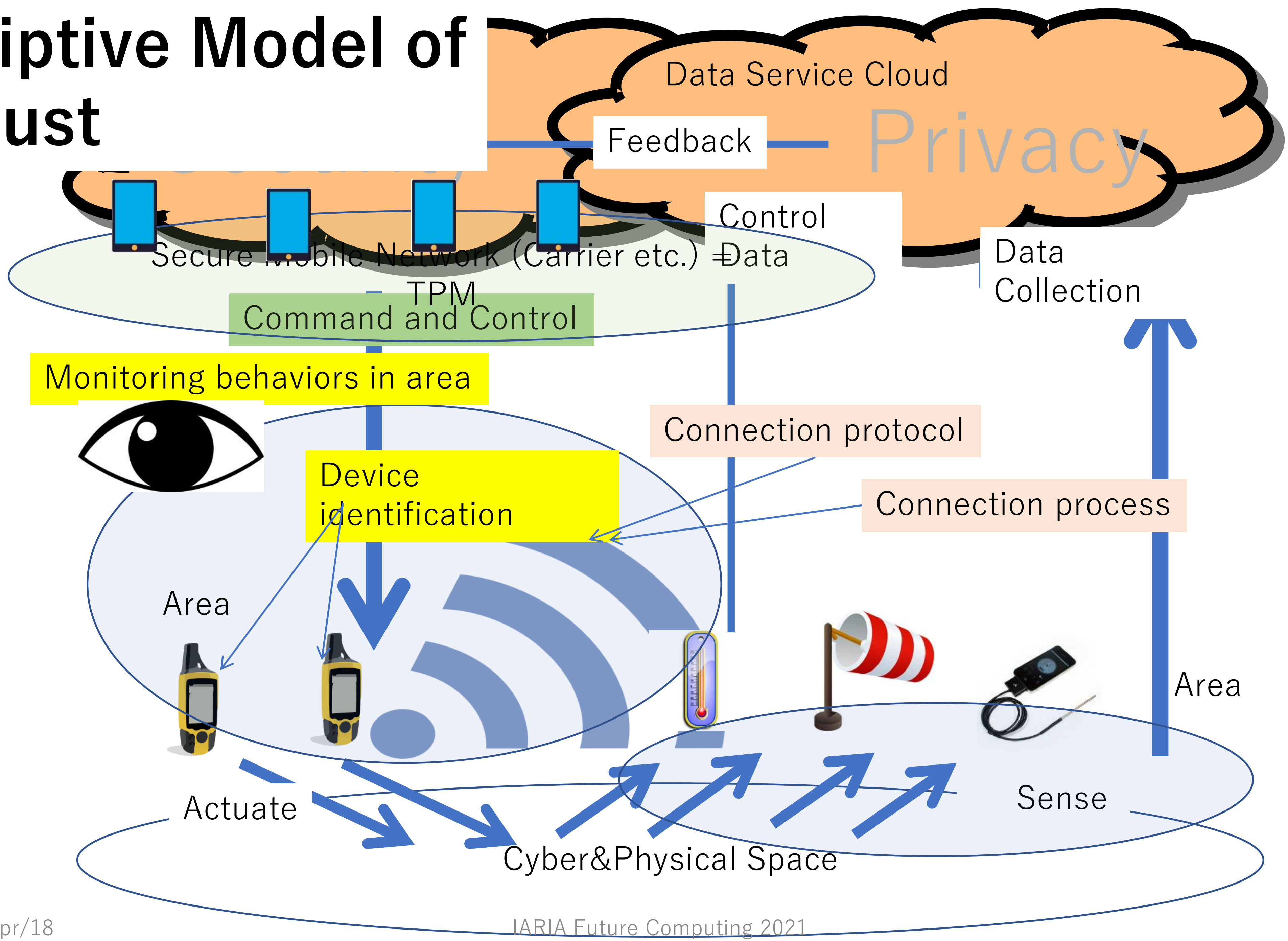
The Point we can control the Behaviors of Nodes.

And Monitoring

- Monitoring of Device Behaviours
  - Instead of identifying individual devices, we MONITOR the area.
    - Same idea as the security in depth.
    - The levels of monitoring matter
- Then, assurance levels for identities → assurance levels for devices

- Monitoring is also used as a real time Audit.

Descriptive Model of IoT Trust



Data Service Cloud

Feedback

Privacy

Control

Secure Mobile Network (Carrier etc.) –Data

– TPM

Command and Control

Data Collection

Monitoring behaviors in area

Device identification

Connection protocol

Connection process

Area

Area

Actuate

Sense

Cyber&Physical Space

Model of IoT Trust

- IoT Trust is Elastic
  - When necessary, we invest devices, and enlarge the trusted area
  - When a project is shut down, we throw away devices and shrink the trusted area

- It is necessary to represent this dynamic behaviors of Trust.

- → Elastic Trust Model

Elastic Trust Model – Analytical [4]

- Let us consider a simple formulation of PDP (Policy Decision Point)

- An entity *e* has its own policy decision engine PDP $|=e$
  - *A*, A set of assertions
  - Assertions are of the form [assert(f, P)] (entity f claims P)
  - When a decision engine $|=e$ judges a policy *P* is valid with a set of assertions *A*, we write
    - $A \,|{=}e\; P$

- There are a number of entities *e*, and they independently make judgements. Entities exchange data in a distributed environment.

Assertions and Policies

- Entity *e* has *trust,* a set of entities that *e* trusts their assertions, that is $\{(f, [\mathrm{assert}(f, P)]) \mid f\colon \text{entity}, P\colon \text{property}\}$ meaning that entity *e* trust that entity *f* claims *P*.
- If $A \ni [\mathrm{assert}(f, P)]$, and $(f, [\mathrm{assert}(f, P)])$ is trusted, then $A \,|{=}\, e\ \ \mathrm{assert}(f, P)$ and $A \,|{=}\, e\ P$

- Assertions (exchangeable data) → Policy (target of judgement)

Trust PDP

- In exchanging data, *e* may receive a set of assertions *B*.
- If A → A ∪ B, *e* make judgements under a new set of assertions.
- Of course *e* has its own acceptance logic of assertions.

- This is a meta engine of PDP → Trust PDP
  - Trusted entities may join and leave
- By using this scheme, we can express elastic trust.

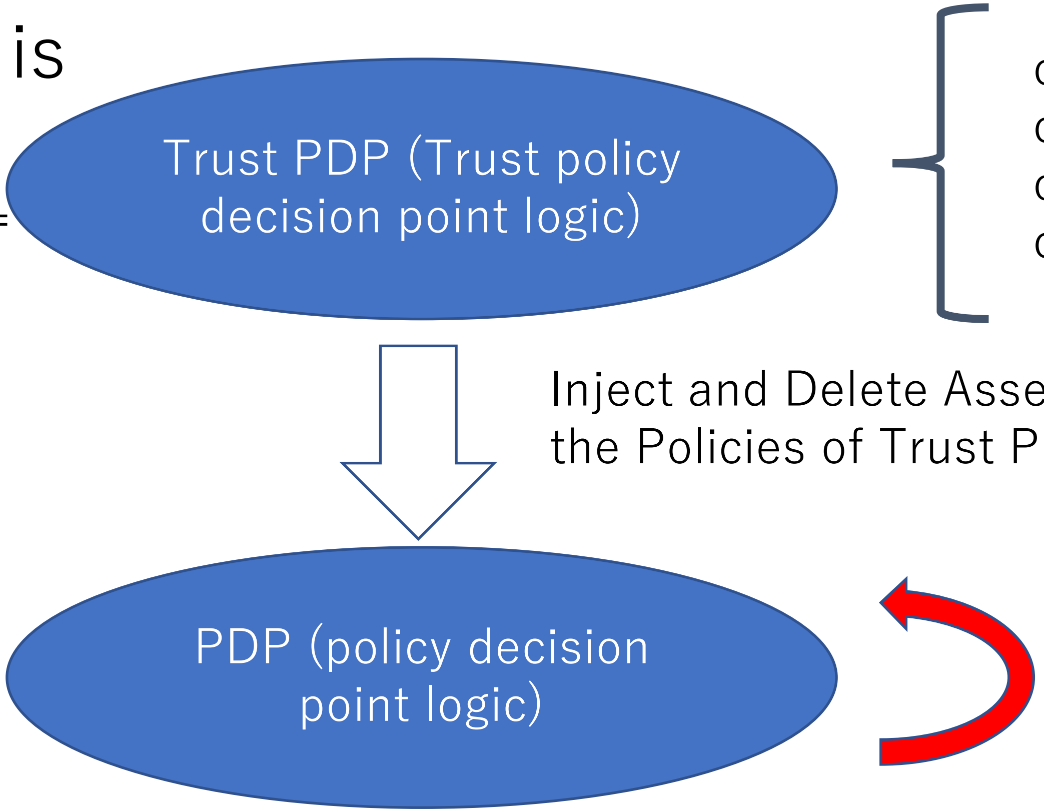
Show by Example

- Trusted entity e scatters sensors s with TPDP trust (e, T) and issues assertions [assert(e, [created(e, s), T])] and [assert(e, [join(s, T)])].

- Another entity d trusts e.
- When d receives [assert(e, [join(s, T)]), s will be added as a trusted entity for d.
- Sensor s sends data [assert(s, [sensed=x])].
- When d receives it, the sensed data x will be trusted.

- We need two-stage logic for elastic trust
- Logic on Trust is important.

Meta-logic of PDP =


Trust PDP (Trust policy decision point logic)
PDP (policy decision point logic)

o trust (e, P)
o create(e, c)
o join(e, T)
o leave(e, T)

Inject and Delete Assertion Sets according to the Policies of Trust PDP

o Usual Logic is available
o When receives an assertion from other parties, accepts or denies it according to the policy given by TPDP.

Show by Example

- Shutdown by monitoring
  - Monitoring may affect the trust scenario of an entity
  - Decision by itself, or Order from Commander
- Blockchain-like node-join
  - Nontrivial trust decision logic (decision by major)
  - Nodes voluntarily join and leave the environment

Concluding Remarks

- In the Internet, Trust plays a major role in extending business
- In classic scenarios, building service federation is supported by trust framework, and we see some deployment

- In near future, Trust will be stratified, and we will see overlay over the same Internet infrastructure.
  - High-Value data and computing resources require high-value trust in identities
  - Technical solutions (security, authentication, …) are now ready, and we will see deployment of new kind of trust framework.
- Another topic to discuss would be on new network environment: IoT, highly decentralized network.
  - We have first shown a descriptive model of IoT trust (with wireless communications). Area trust and monitoring are critical components.
  - Next, we have shown an analytical model of IoT trust – elastic trust model.

References

[1] NIST, Digital Identity Guidelines, NIST SP800-63(-3), 2017.

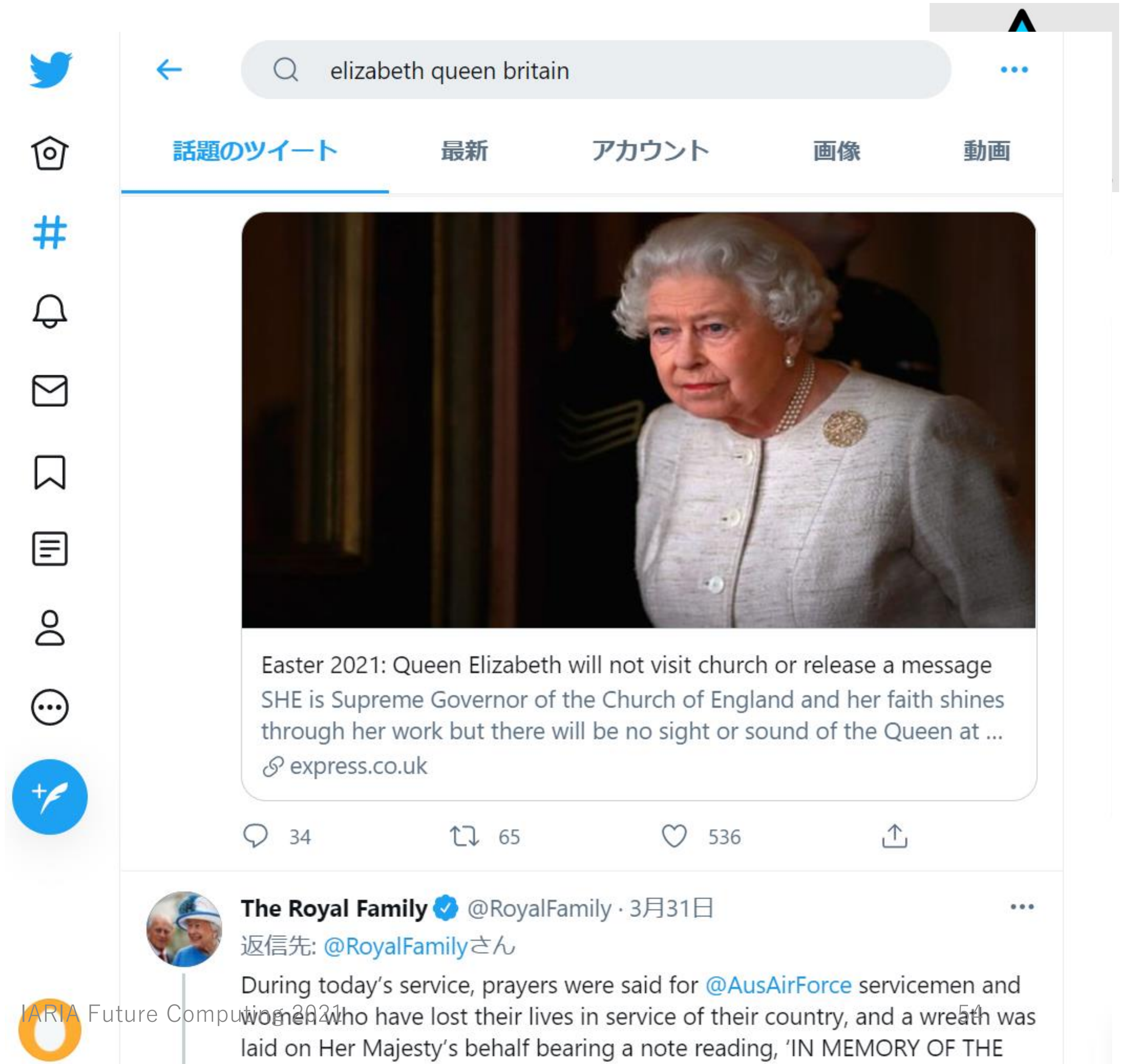
[2] NIST, Zero Trust Architecture, NIST SP800-207, 2020.

[3] Sato, H. et.al.: Establishing Trust in the Emerging Era of IoT, Proc. IEEE Int'l Conf. Service-Oriented System Engineering 2016 398—406, 2016.

[4] Sato, H. Yamamoto N.: Elastic Trust Model for Dynamically Evolving Trust Frameworks, IEICE Trans. Information Systems, Vol. E102-D, 1617—1624, 2019.

Thank you!

- Even press and gossips…
  (under the name of SNS)



Easter 2021: Queen Elizabeth will not visit church or release a message
SHE is Supreme Governor of the Church of England and her faith shines through her work but there will be no sight or sound of the Queen at ...
express.co.uk

The Royal Family @RoyalFamily · 3月31日
返信先: @RoyalFamilyさん
During today's service, prayers were said for @AusAirForce servicemen and women who have lost their lives in service of their country, and a wreath was laid on Her Majesty's behalf bearing a note reading, 'IN MEMORY OF THE

How Identity Assurance is Guaranteed

- [Trust Framework] Define Policies of operations
- [Trust Framework] Publish the policies (criteria) of identity assurance
- [IdP and SP] Join the trust framework with the Contract
- [SP] Trust IdPs, assuming the operations of IdP are compliant with the published policies
- [Trust Framework] (Regularly) Assess the operations of IdPs and SPs as the compliance audit

- Emergence of **Internet Trust Engineering**
  - **Security, authentication**
  - **Building Framework**
  - **Policy analysis and enforcement**
  - …