Intel
Confidential

Strong Authentication in the Cloud

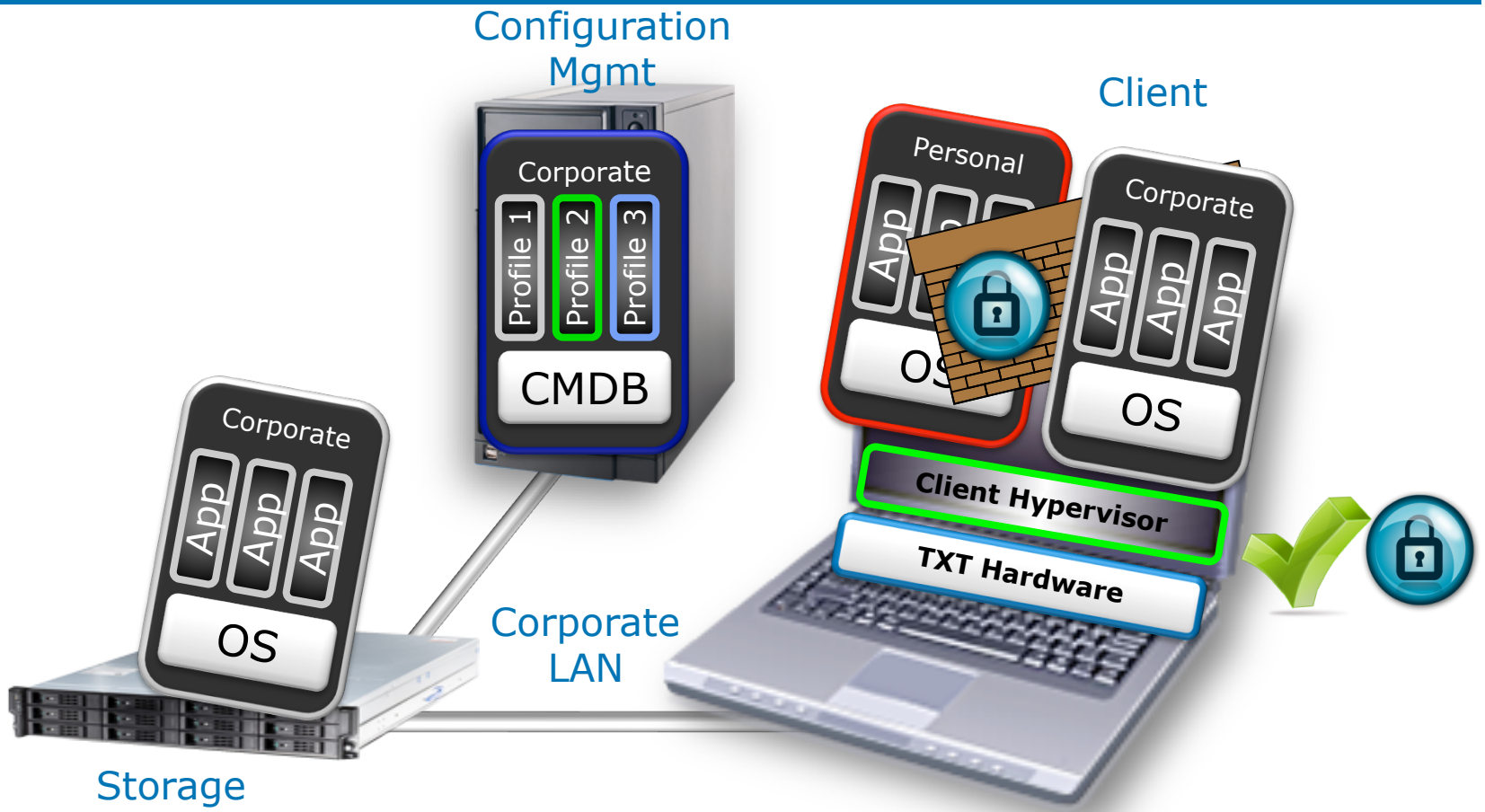
Ned Smith
Intel

Agenda

- Cloud use cases
- Private Cloud
- Public Cloud
- Multi-Tenancy
- Identity Management
- Deployment Considerations
- Conclusion

Spectrum of Cloud Hosting Models

Private Cloud Hosting Model for Client-side Virtual Container



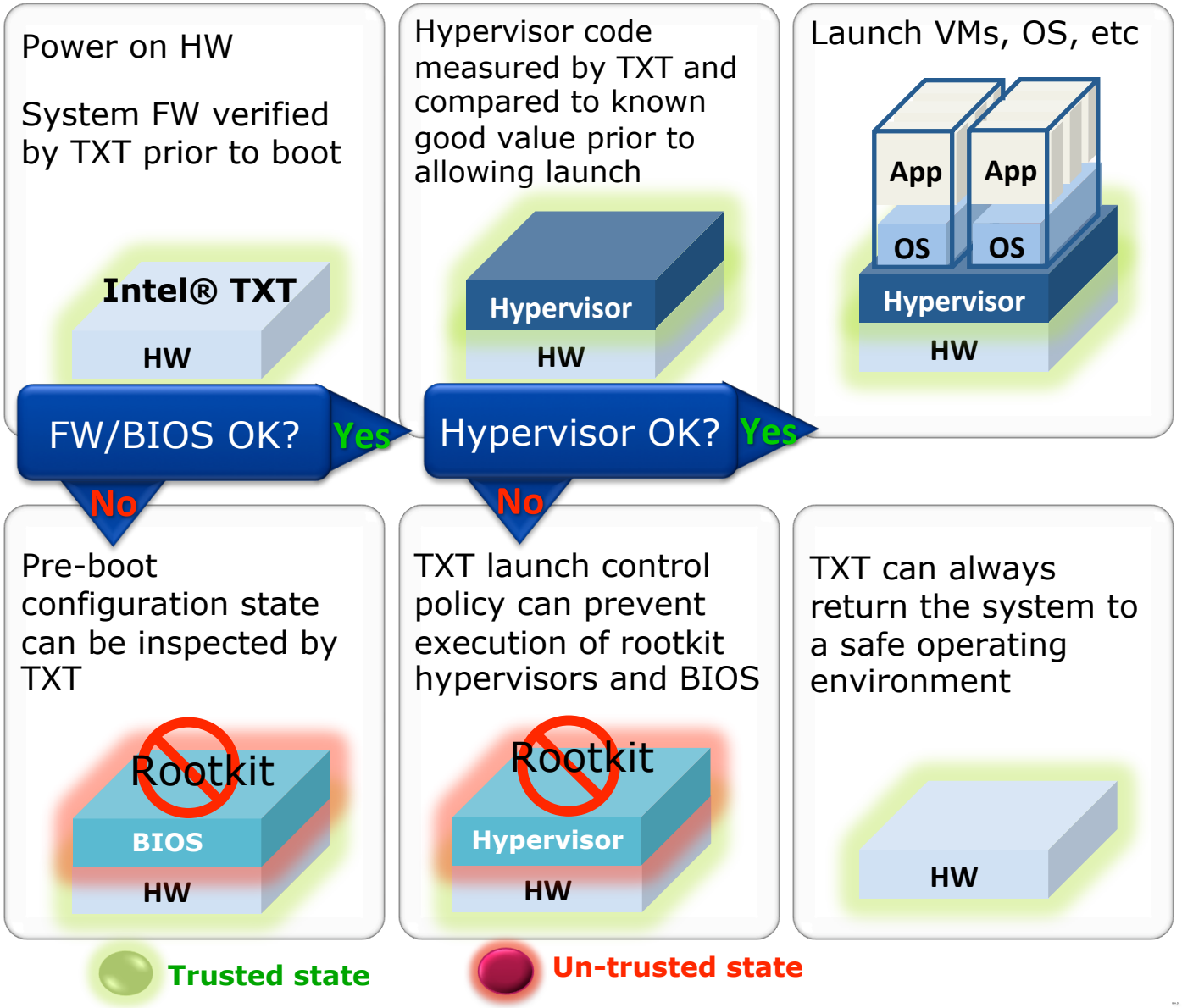
IT Experience is Centralized Security & Control

User Experience is Responsiveness, Mobility & Protection

Private Cloud Attestation

With Intel® TXT:
Software can be measured and verified as known good

…and tampering can be detected or blocked



Public Cloud Hosting Model for Virtual Containers (IaaS)

Cloud Experience is Consistent Security & Control of Hosting Environment

User Experience is Mobility, Availability, Control of Application Environment

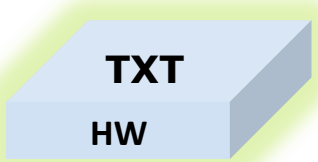
Public Cloud Attestation

With TXT: Service Provider can verify hosting environment is good

…and Subscriber attestation proves SP environment is acceptable before releasing sensitive data

Power on HW

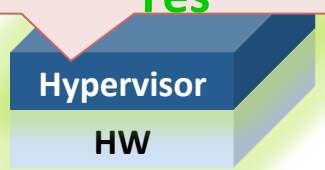
Intel® TXT measures BIOS and SMM



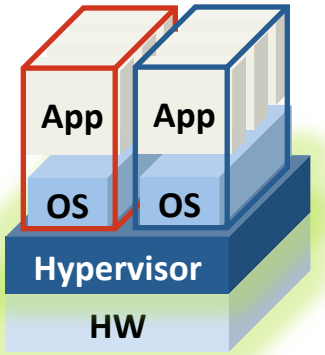
The TXT Authenticated Code Module measures hypervisor and compares to known good value

HYP, SMM, BIOS match?

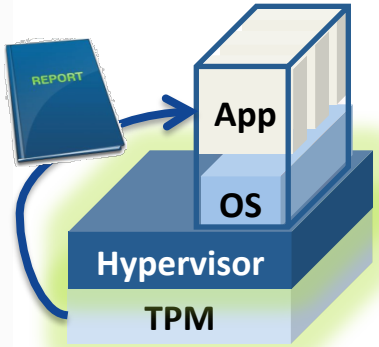
Yes



Launch VMs, OS, etc

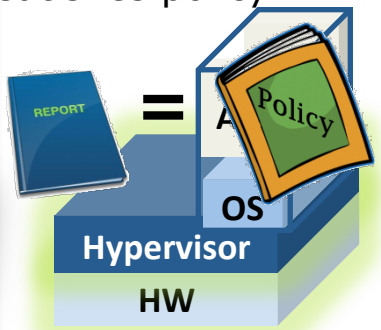


Hosted app obtains attestation report



Hosted app forwards report to cloud subscriber

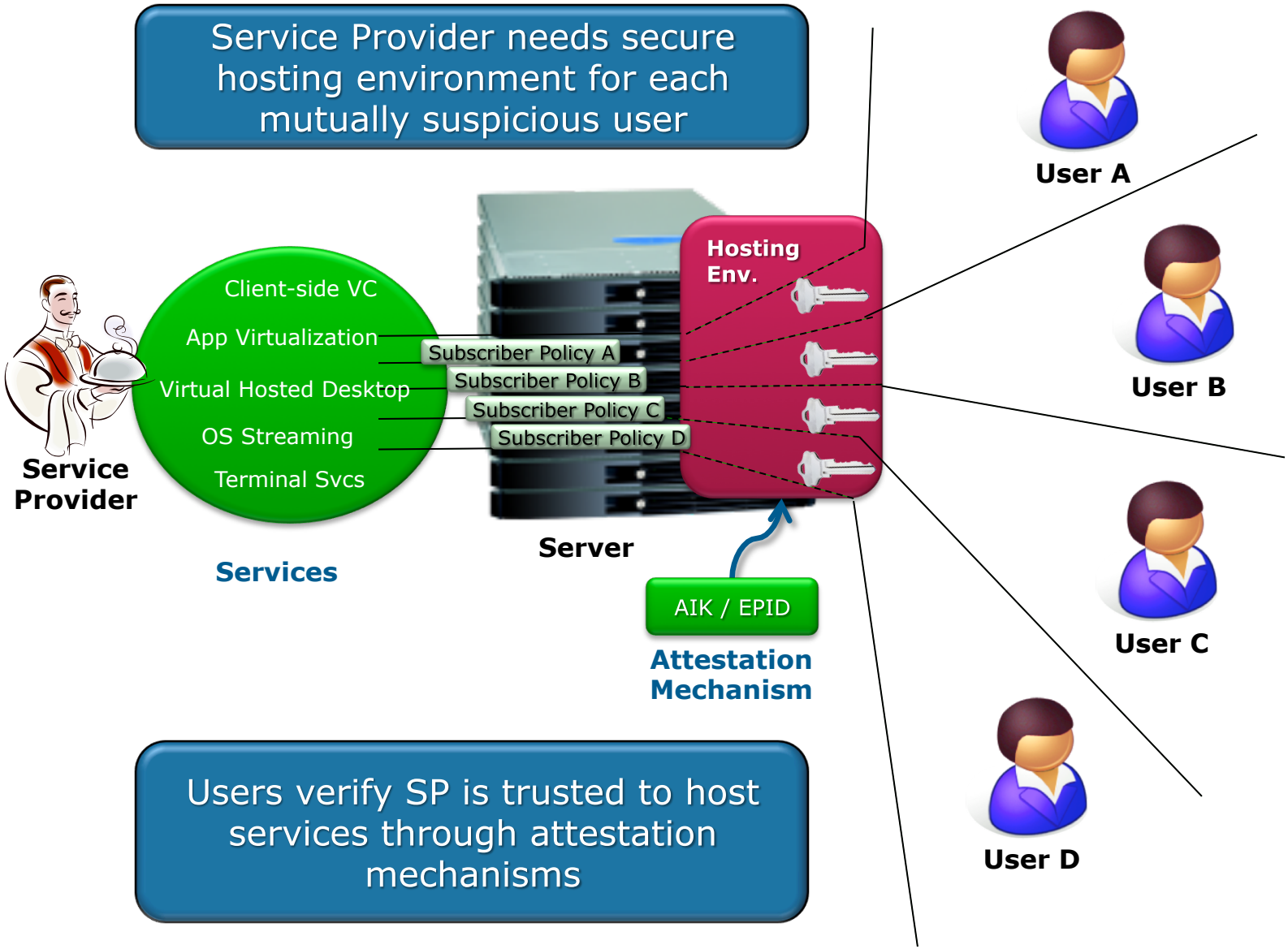
Subscriber verifies reported hypervisor satisfies policy



Cloud Depends on Multi-Tenancy

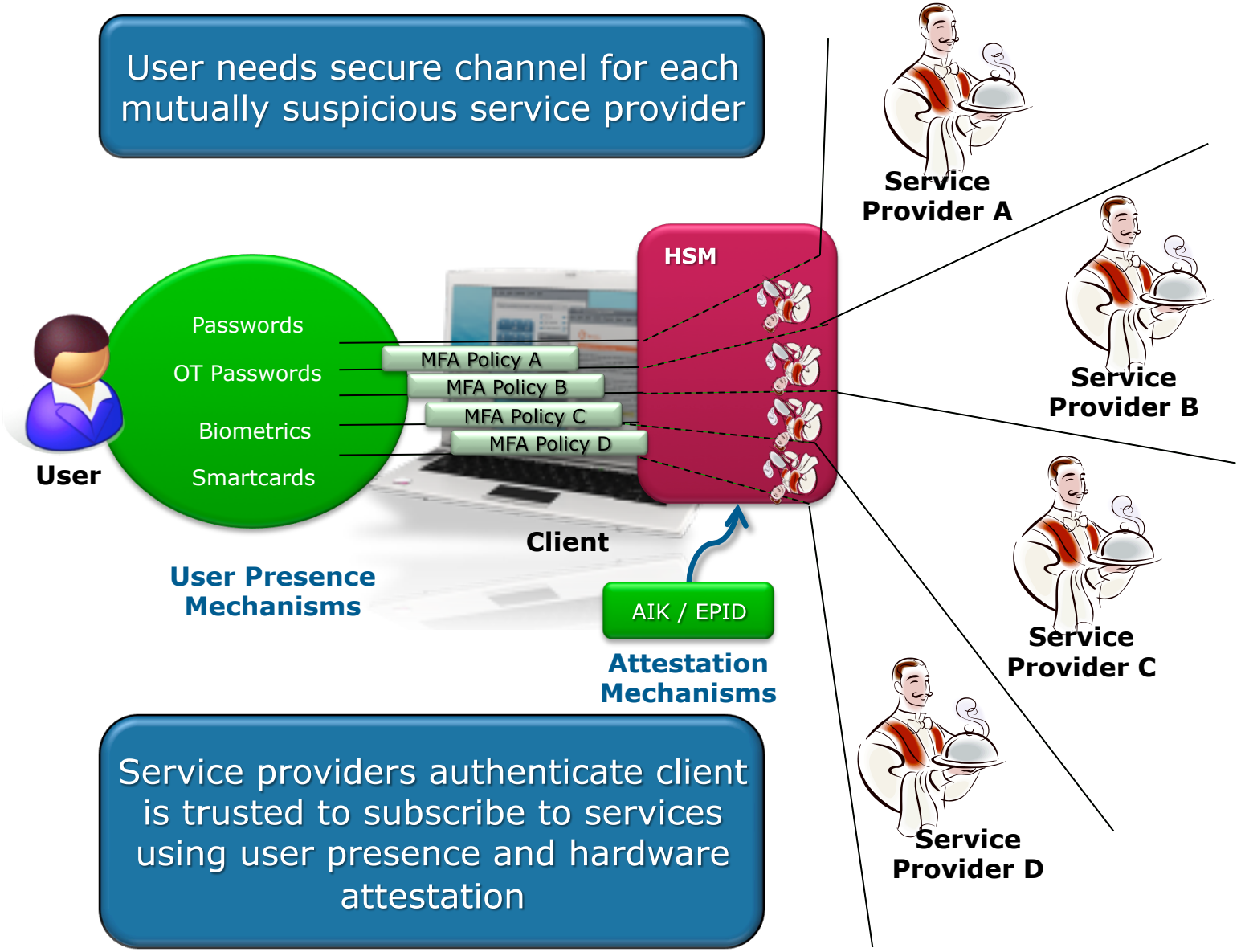
- Service providers may have multiple subscribers
- Cloud subscribers may contract with multiple service providers
- "Mutually suspicious" security semantics
- Requires
  - User and service provider authentication
  - Server and client environment attestation

Multi-tenancy for Service Providers



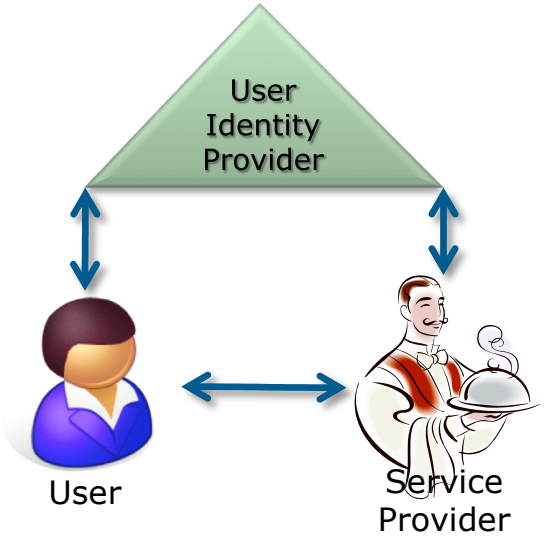
Multi-tenancy for Clients

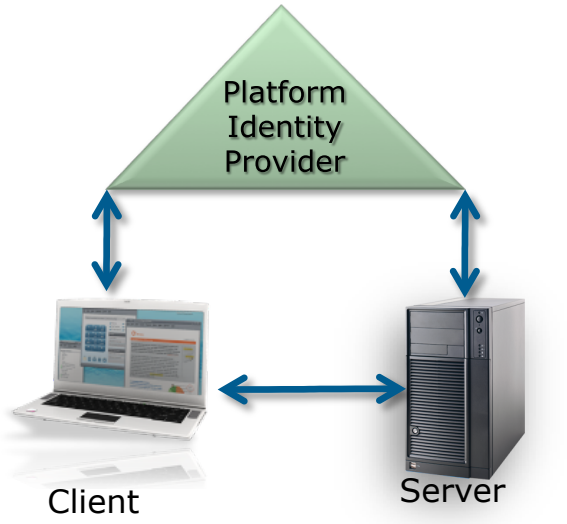
User needs secure channel for each mutually suspicious service provider



Service providers authenticate client is trusted to subscribe to services using user presence and hardware attestation

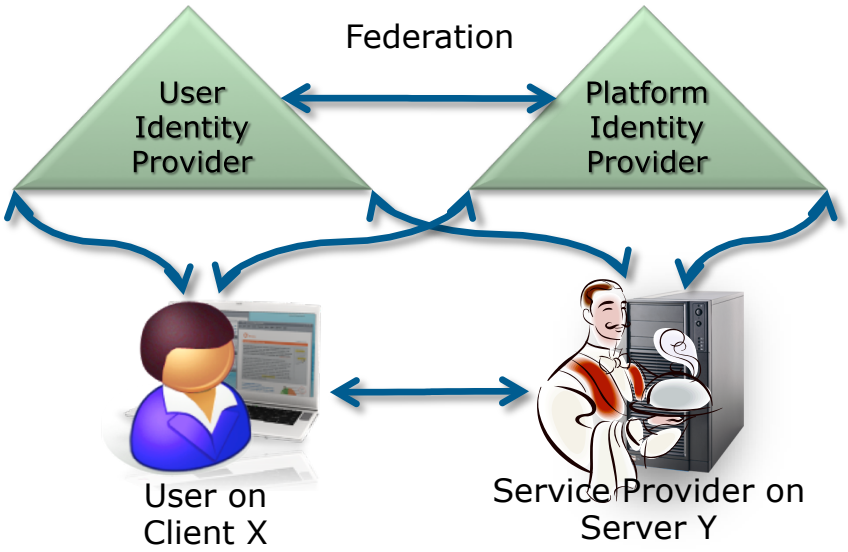
Today User and Platform Identity Management are Separated





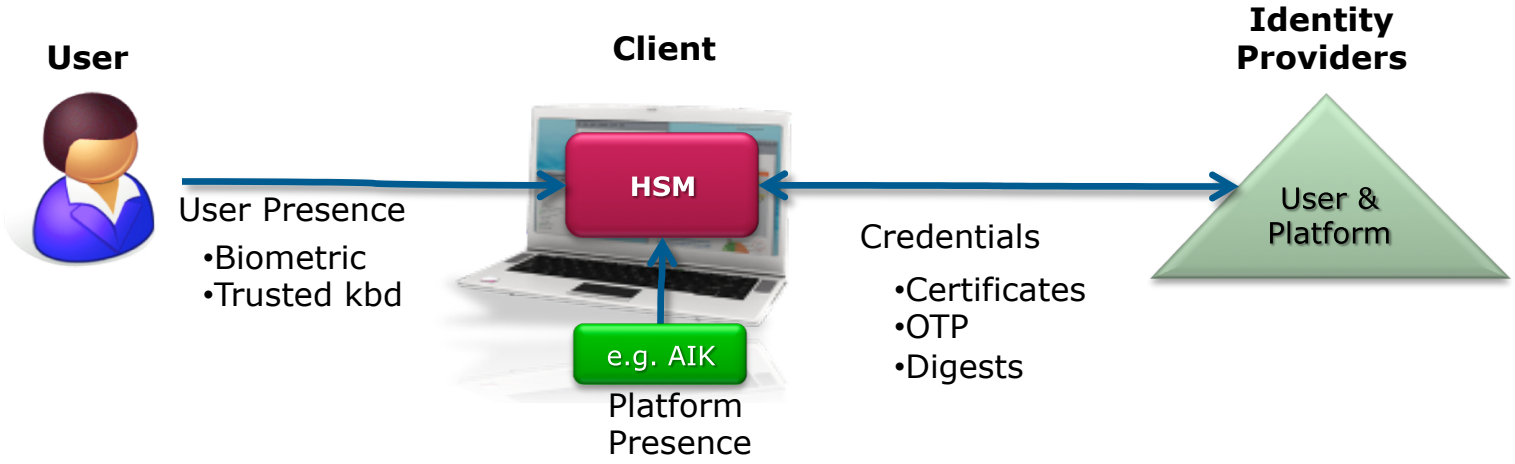
- User Identity Examples
  - Kerberos KDC - tickets
  - Certificate Authority – X.509 certificates
  - Web service / Open ID – password digests
- Platform Identity Examples
  - TCG Privacy CA - AIK certificates
  - TLS – "Machine certs"
  - EPID Mfg CA (more later)

Cloud Models Suggest Integrated Identity Management



- User identity believability improves when coupled with platform identity
- Platform identities are (can be) provisioned at manufacturing time
  - Addresses "step-0" problem
- Common framework for identity management deployment lifecycle

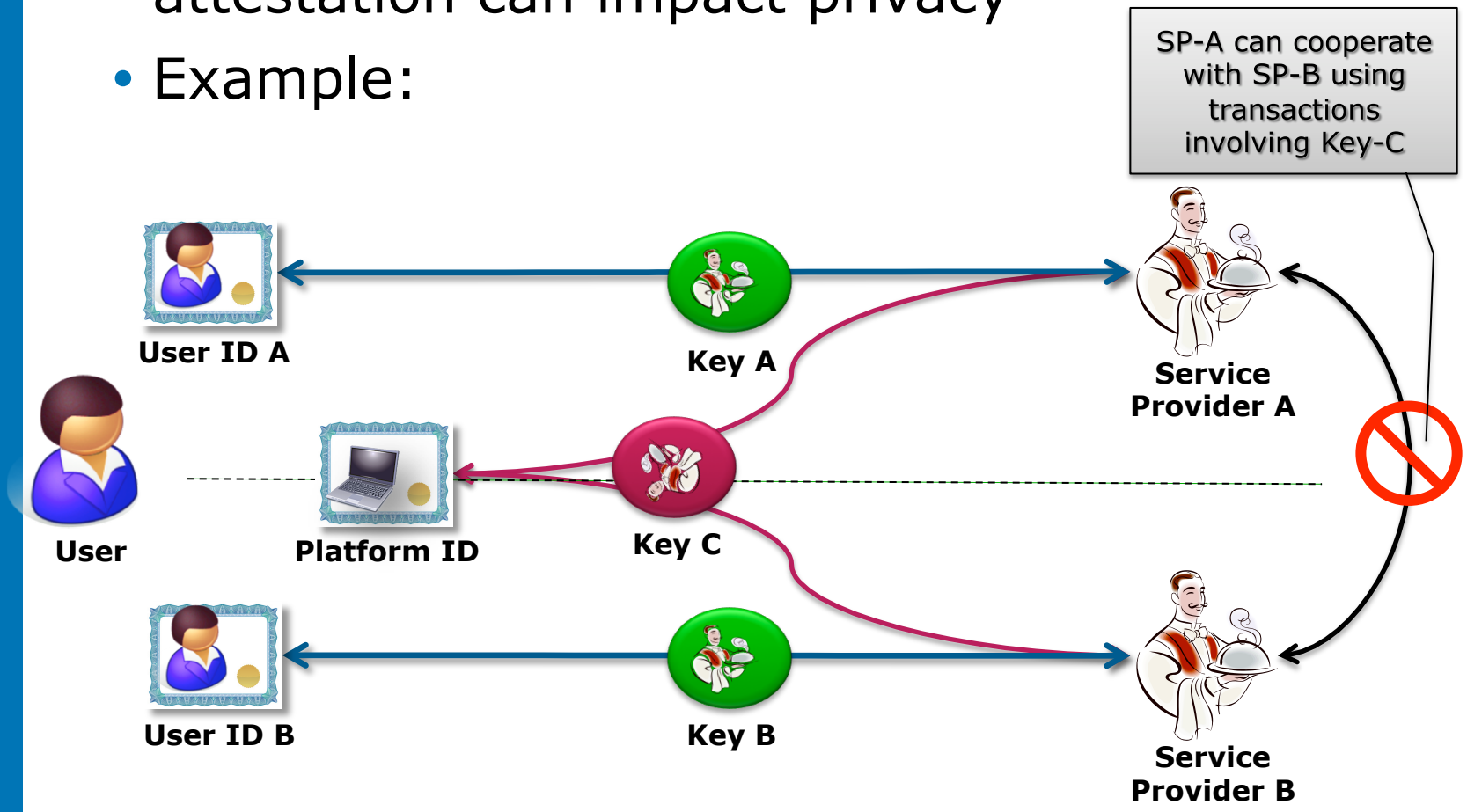
What Makes User Identity Believable?



- User must authenticate reliably
- Identity provider must prove this occurred
- Properties:
  - Hardened attestation module (e.g. TPM)
  - Hardened user authentication module (e.g. HSM)
  - Integration

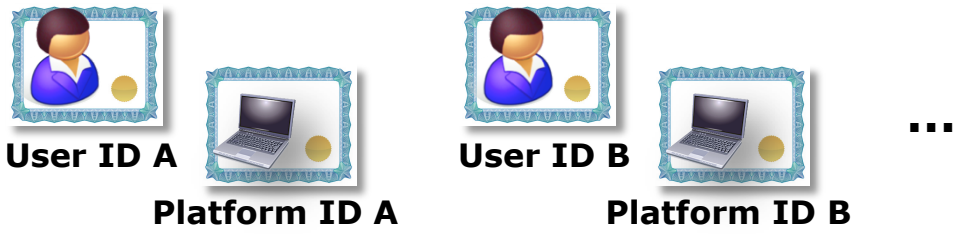
What about Privacy?

- Integration of user authentication with attestation can impact privacy
- Example:

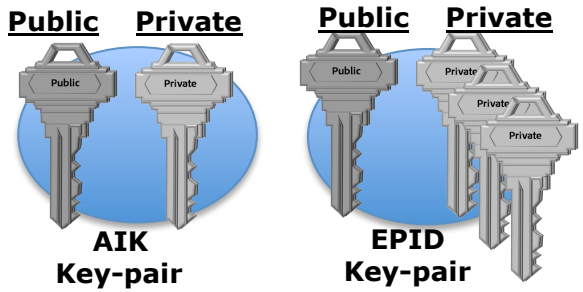


Possible Solutions for Privacy Enhanced Platform IDs

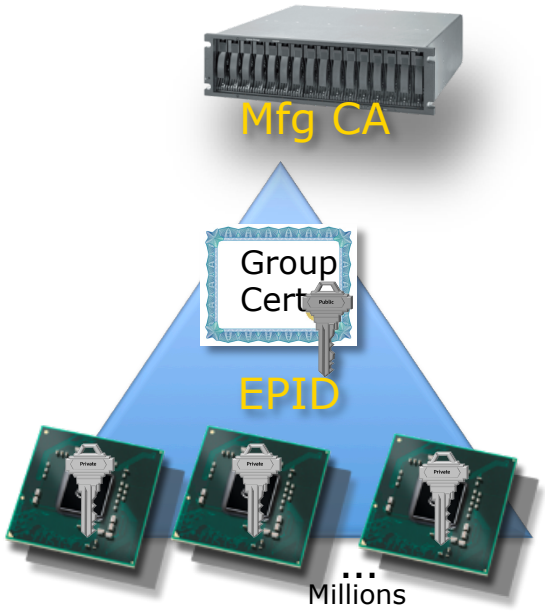
- TCG Attestation Identity Keys (AIK)
  - For each user identity, use a unique AIK
    - Traditional asymmetric key pair is 1-to-1
  - E.g.



- Privacy Enhanced Identifier (EPID)
  - For each user identity, use the same EPID key
  - EPID is 1-to-many; one public key, many private keys
  - Privacy is enhanced with greater number of private keys



EPID Manufacturing

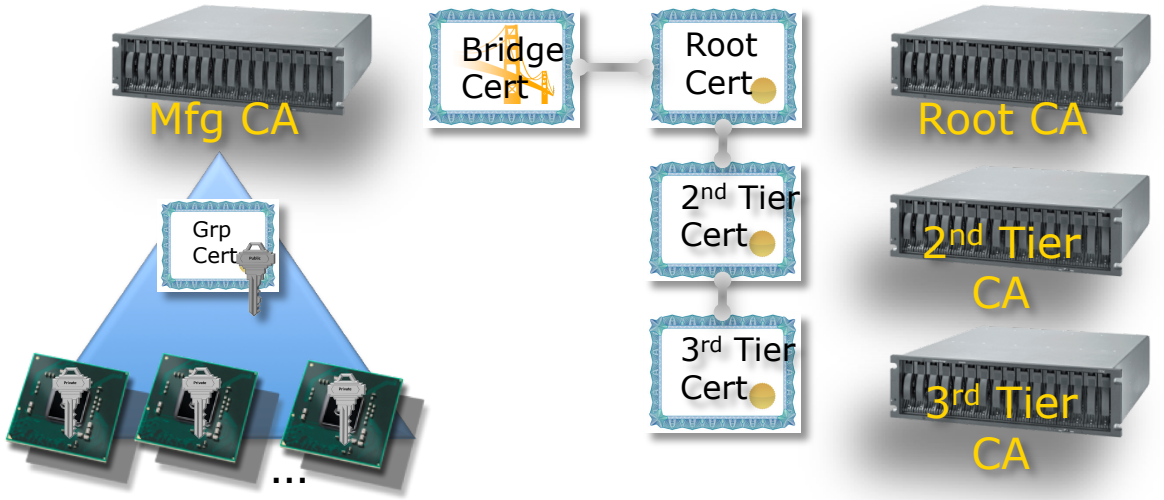


- A unique private key is assigned to each platform
- A new group is started after several million private keys have been assigned
- Manufacturer CA issues a "group" certificate based on the single public key associated with the group

Privacy is preserved because Service Provider A cannot correlate use of EPID when used with Service Provider B

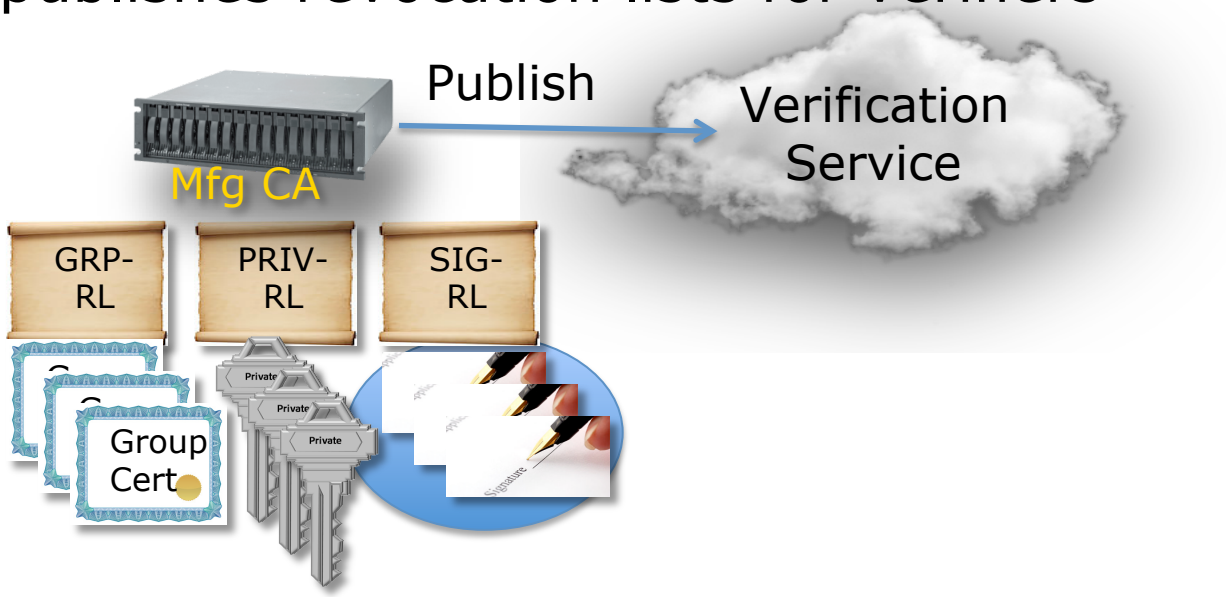
EPID Certificate Model

- Traditional CA has 2 or 3 tiers
- The root CA public key terminates certificate path validation
- Manufacturing CA issues a "Bridge Cert" allowing path validation beyond traditional root CAs



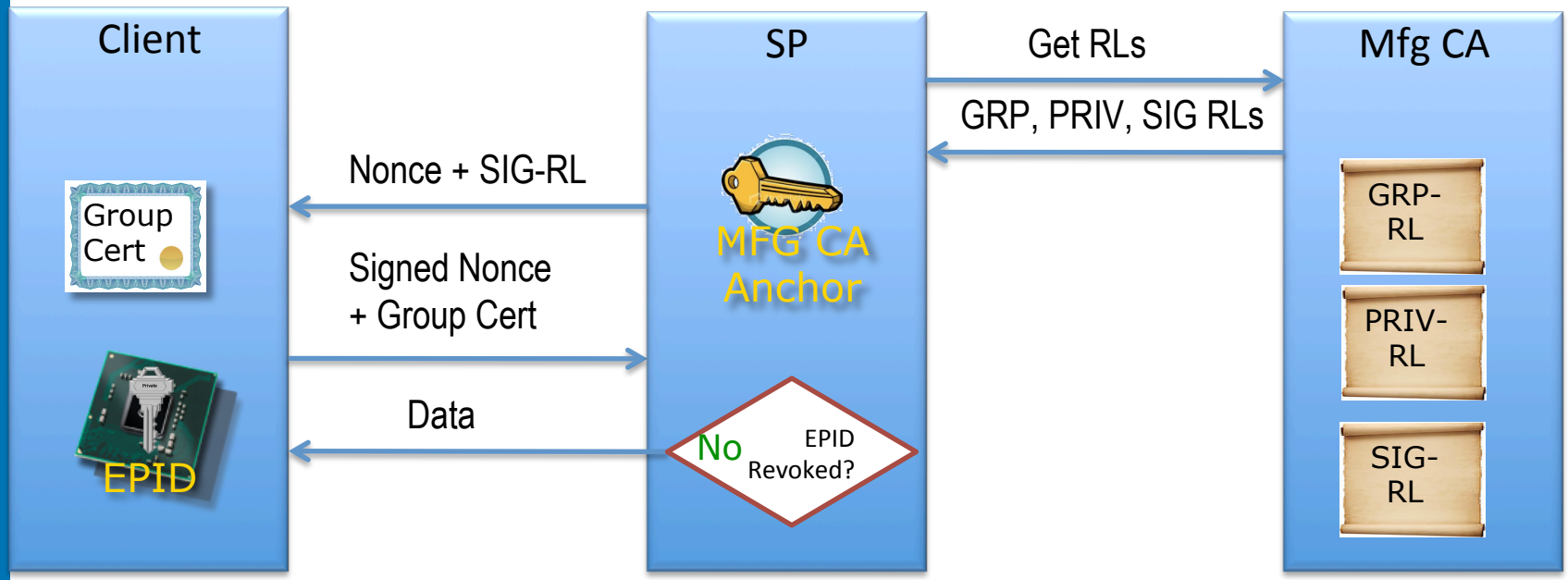
EPID Revocation

- Traditional PKI use a Certificate Revocation List (CRL) to identify revoked certificates
  - Existence of public key implies revocation of private key
- EPID has 3 revocation lists
  - Grp-RL : Uses public key to revoke all private keys
  - Priv-RL : A specific private key may be revoked
  - Sig-RL : A private key signature may be revoked
    - EPID signing must include Sig-RL as input
- Mfg CA publishes revocation lists for verifiers



EPID Verification

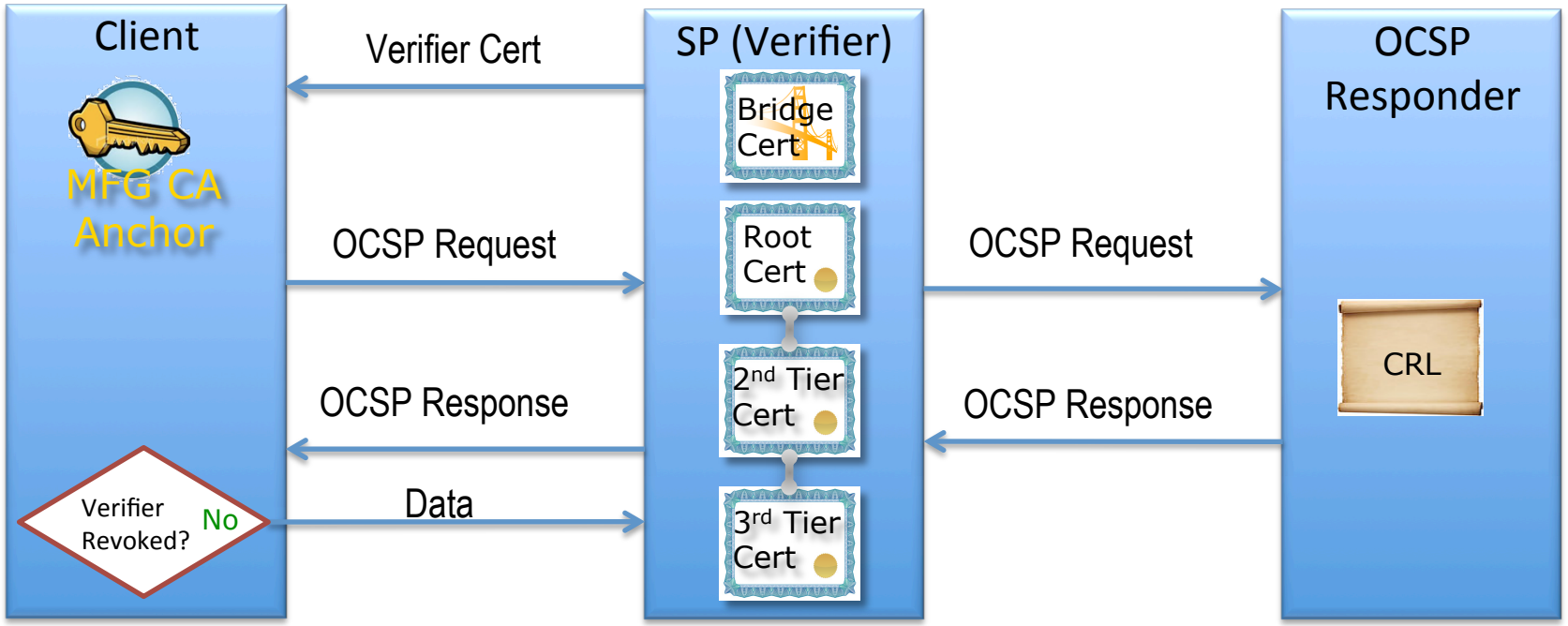
- Sigma is a signed Diffie-Hellman key exchange protocol that uses EPID to sign
- EPID verification flow:



- Verifier is provisioned with Mfg CA anchor key
- Verifier is extended to support EPID revocation
- Verifier must obtain fresh SIG-RL for each use of EPID

Verifier Verification

- Verifier certificate verification flow:



- Verifier is provisioned with both Bridge Cert and traditional cert chain
- Mfg CA anchor key is provisioned during manufacturing

Status of EPID

- EPID is accepted by ISO/IEC 20008-2
  - "Anonymous Digital Signatures" draft
  - http://www.iso.org/iso/catalogue_detail.htm?csnumber=57018
  - Co-chairs
    - Jiangtao Li – Intel
    - Kazue Sako - NEC
- Other presentations on EPID
  - http://www.trust2010.org/slides/Li.pdf

Conclusion

- Cloud multi-tenancy requirements apply to both servers and clients
- Identity management infrastructure needs to unify user and platform identities
- Cloud service providers and subscribers rely on bi-lateral attestation to gauge veracity of the other's environment
- EPID is a platform identity that satisfies privacy requirements and may be cost effective to manufacture