SDC
STORAGE DEVELOPER CONFERENCE
SNIA SANTA CLARA, 2016

Cloud Access Control Delegation

David Slik
NetApp, Inc.

Cloud Risks & Rewards

- The use of cloud-based data storage has significant technical and business value:
  - Economic "as-a-service" consumption
  - Geographic diversity & mobility
  - Proximity to cloud compute resources

- However, cloud-based data storage introduces significant legal and operational risks:
  - Maintaining data ownership and controls
  - Preventing unauthorized data access

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Cloud Risks & Rewards

- These areas of concern have limited the adoption of cloud-based data storage outside situations where:
  - Data is already public
  - Unauthorized disclosure has little economic or political consequence
  - Unauthorized disclosure can be blamed on or consequences transferred to other actors (such as the cloud provider)
  - Costs of avoiding risks are higher than costs of the consequences of the risks

Cloud Risks & Rewards

- Encrypting data before storing it into the cloud resolves governance and access control concerns, but introduces significant new issues:
  - Need to build an entirely new access control and key management system (KMS) + key distribution infrastructure, and modify clients to use these
  - Cloud resources can no longer access data directly, and data needs to flow through custom code that talks with the KMS and decrypts data

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Cloud Risks & Rewards

- Ideally, a solution to these trade-offs would involve:
  - Not significantly increasing costs, as this would negate economic benefits of cloud-based data storage
  - Not requiring modifications to cloud infrastructure, which is often not possible because it is controlled by third-parties
  - Require limited or no modifications to applications

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Introducing SNIA DAC

DAC – Delegated Access Control

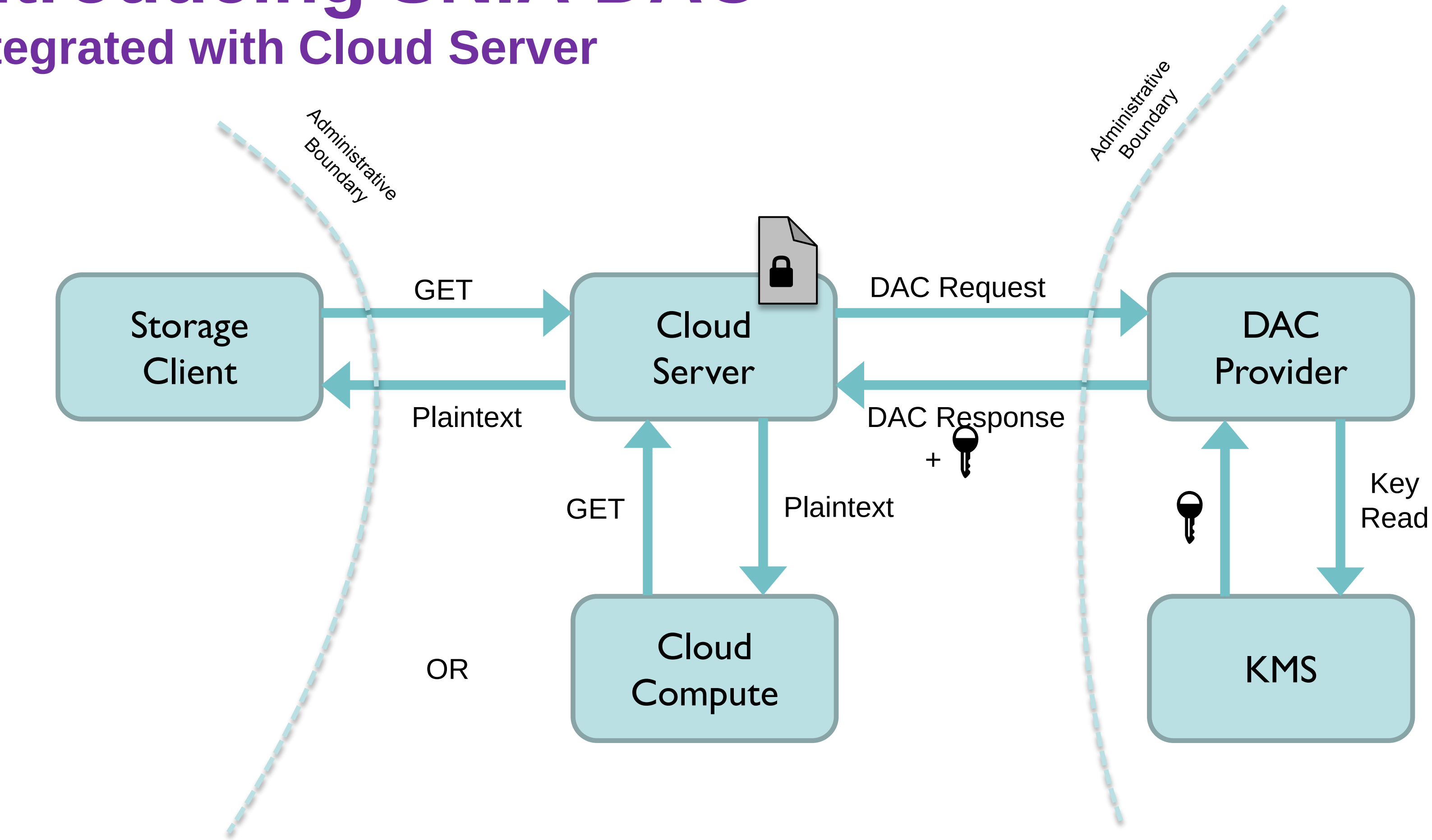
- Standardizes a simple challenge/response protocol for delegating access control decisions and key distribution for HTTP-based storage
- Started as CDMI extension, but works with S3, Swift, etc.

- Can be integrated into any HTTP-based storage protocol
  - Allows use by unmodified clients
  - Allows transparent integration with cloud computing
- Can be used directly by clients
  - Allows use with clouds that don't support DAC

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Introducing SNIA DAC

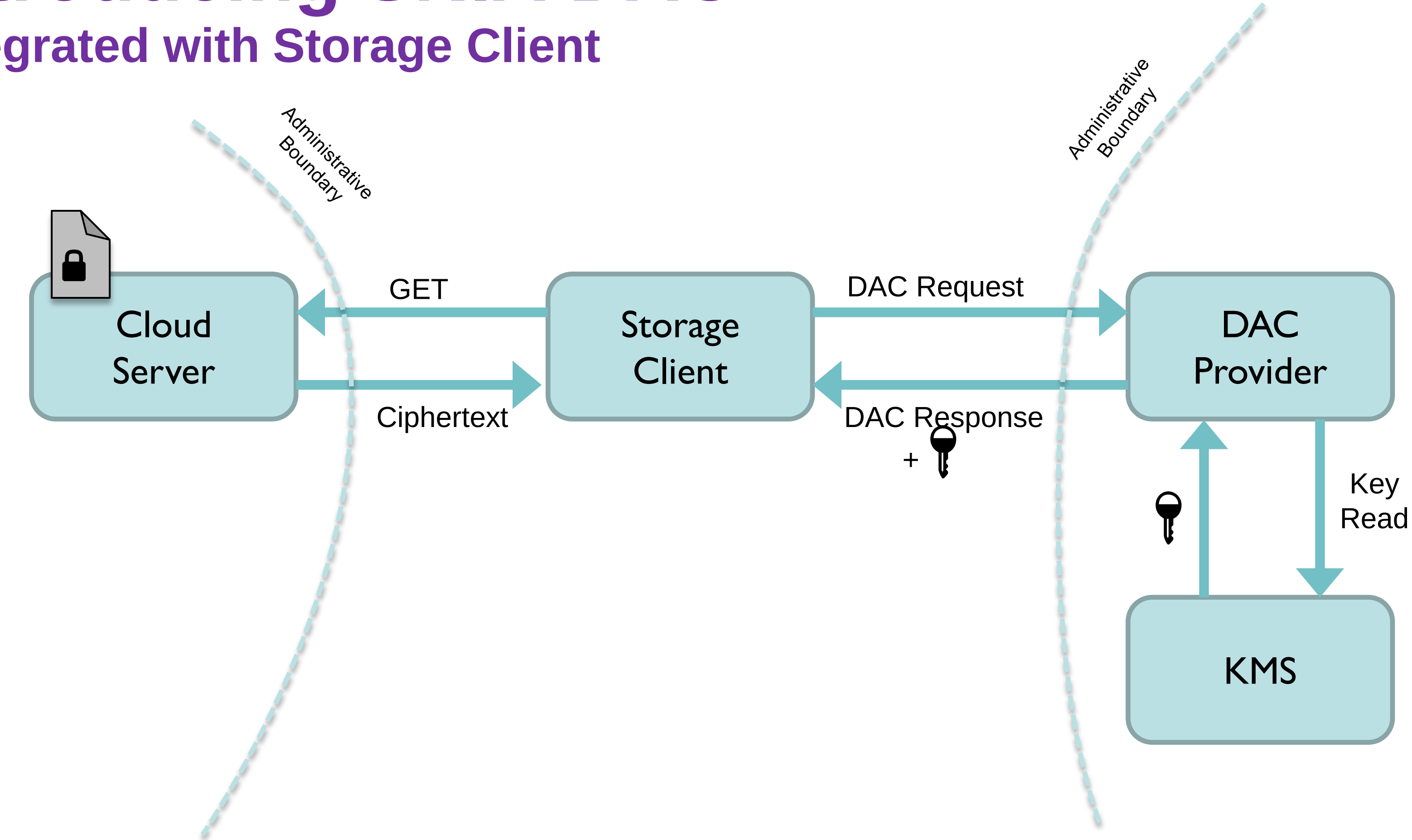
Integrated with Cloud Server



2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Introducing SNIA DAC

Integrated with Storage Client



2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Trustworthy Cloud

- A cloud service that provides assurances (Legal, technical, reputation, audit, etc) that directives on data governance and access control will be honored.
  - Cloud permitted to access to the decryption keys
  - Cloud can thus access data plaintext
- Advantages
  - Allows unmodified clients
  - Allows cloud-driven data processing
- Disadvantages
  - Does not protect against a malicious cloud
  - Does not protect against a compromised cloud

Untrustworthy Cloud

- A cloud service that is known, suspected or capable of violating data governance and access control directives due to technical, financial or personnel issues.
  - Cloud not permitted to access decryption keys
  - Cloud cannot access data plaintext
- Advantages
  - Does not require modifications to cloud
  - Protects against malicious and compromised clouds
- Disadvantages
  - Requires client modifications or proxy
  - Does not support cloud-driven data processing

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Delegated Access Control Landscape

	Untrustworthy Cloud	Trustworthy Cloud
Access Control Performed by Cloud	Client DAC Required for Trust	Server DAC Or Client DAC Required for Trust
Support for Delegated Access Control	Client DAC Required for Trust	Server DAC AWS KMS

Amazon S3

Microsoft Azure

OpenStack Swift

[1] https://d0.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Additional Integration Points

- Cloud Integration
  - Requires participation of cloud provider
- Client Integration
  - Requires modifications to application
- Web Application Integration
  - Requires less invasive modifications to web apps
- Proxy Integration
  - Requires no modifications to applications

Web Application Integration

Where cloud supports Delegated Access Control

- Javascript library added to web application that intercepts all AJAX calls
  - Library adds headers to cloud HTTP(S) operations
  - Cloud forwards request to Delegated Access Control system
  - Delegated Access Control system makes access determination decision based on client headers
  - Ciphertext returned with access headers
  - Library decrypts access headers
  - Library uses access headers to transparently decrypt ciphertext

Web Application Integration

Where cloud does not support Delegated Access Control

- Javascript library added to web application that intercepts all AJAX calls
  - Library gets ciphertext from cloud HTTP(S) operation
  - Library makes Delegated Access Control request directly to Delegated Access Control system
  - Delegated Access Control system makes access determination decision based on client headers
  - Library decrypts access headers
  - Library uses access headers to transparently decrypt ciphertext

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Native Protocol Proxy Integration

Where cloud supports Delegated Access Control

- Proxy added between application and cloud provider
  - Proxy receives application HTTP(S) operation
  - Proxy adds adds headers to cloud operations
  - Cloud forwards request to Delegated Access Control system
  - Delegated Access Control system makes access determination decision based on client headers
  - Ciphertext returned with access headers to proxy
  - Proxy decrypts access headers
  - Proxy uses access headers to transparently decrypt ciphertext, and returns plaintext to application

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

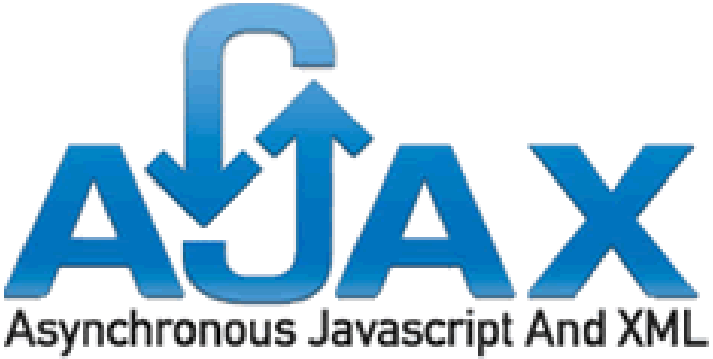
Native Protocol Proxy Integration

Where cloud does not support Delegated Access Control

- Proxy added between application and cloud provider
  - Proxy receives application HTTP(S) operation
  - Proxy gets ciphertext from cloud
  - Proxy makes Delegated Access Control request directly to Delegated Access Control system
  - Delegated Access Control system makes access determination decision based on client headers
  - Proxy decrypts access headers
  - Proxy uses access headers to transparently decrypt ciphertext, and returns plaintext to application

2016 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Demonstration



JavaScript/CDMI Client Demonstration

Call for Participation

- SNIA is widening work on DAC to take it beyond CDMI
- Looking at creating a stand-alone standard for DAC
- If you're working with object/cloud storage, and want to participate, contact us and join the Cloud technical working group (TWG)
  - Weekly Wednesday calls
  - Bi-monthly face-to-face meetings
  - Quarterly plugfests

- Join us at the Plugfest being held at SDC!

Thank you!

Questions

dslik@netapp.com