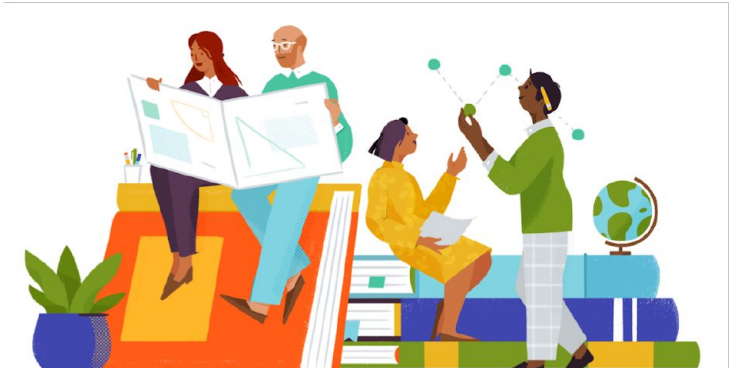
March 27, 2019

# Slack EKM

Richard Crowley
Principal Engineer, Slack



# Slack EKM

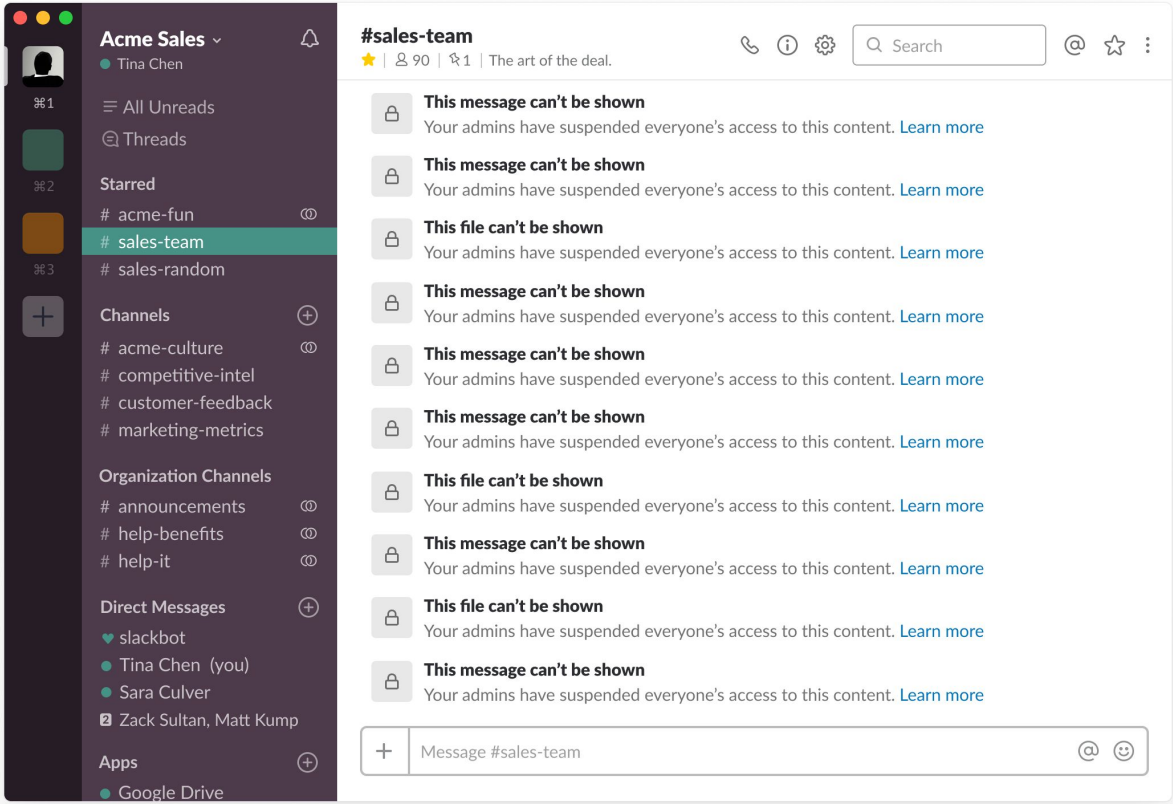
- Integrates Slack with AWS KMS to give our most security-conscious customers control over their encryption keys
- Helps customers manage the risk of relying on a vendor to protect sensitive data and the risk of invisible disclosure

slack

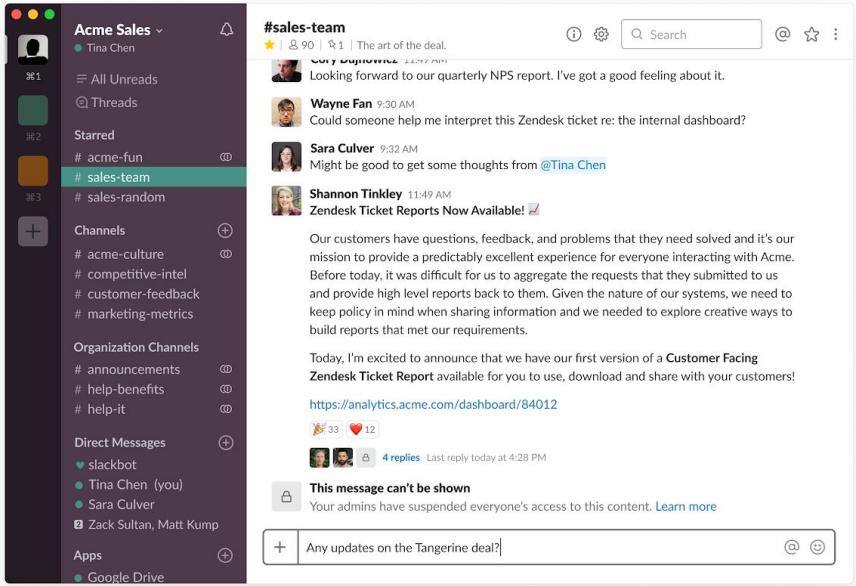
# Slack EKM design objectives

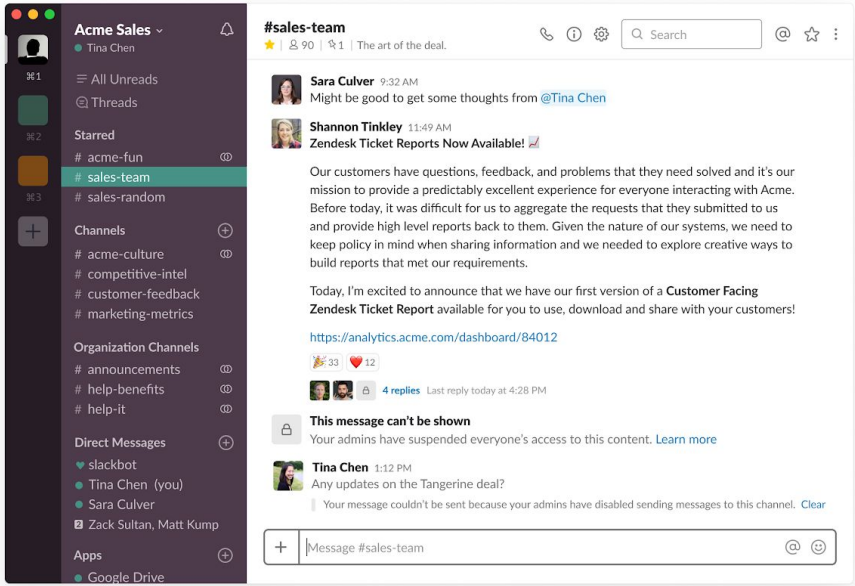
- Slack must remain Slack, feature for feature
- EKM must inspire confidence and earn trust, not merely check a box
- The application’s performance can’t become terrible
- Our engineers must remain productive

# Slack EKM to end users



# Slack EKM to end users




slack

# Slack EKM provides...

**Visibility** into access to the keys that can decrypt your messages and files

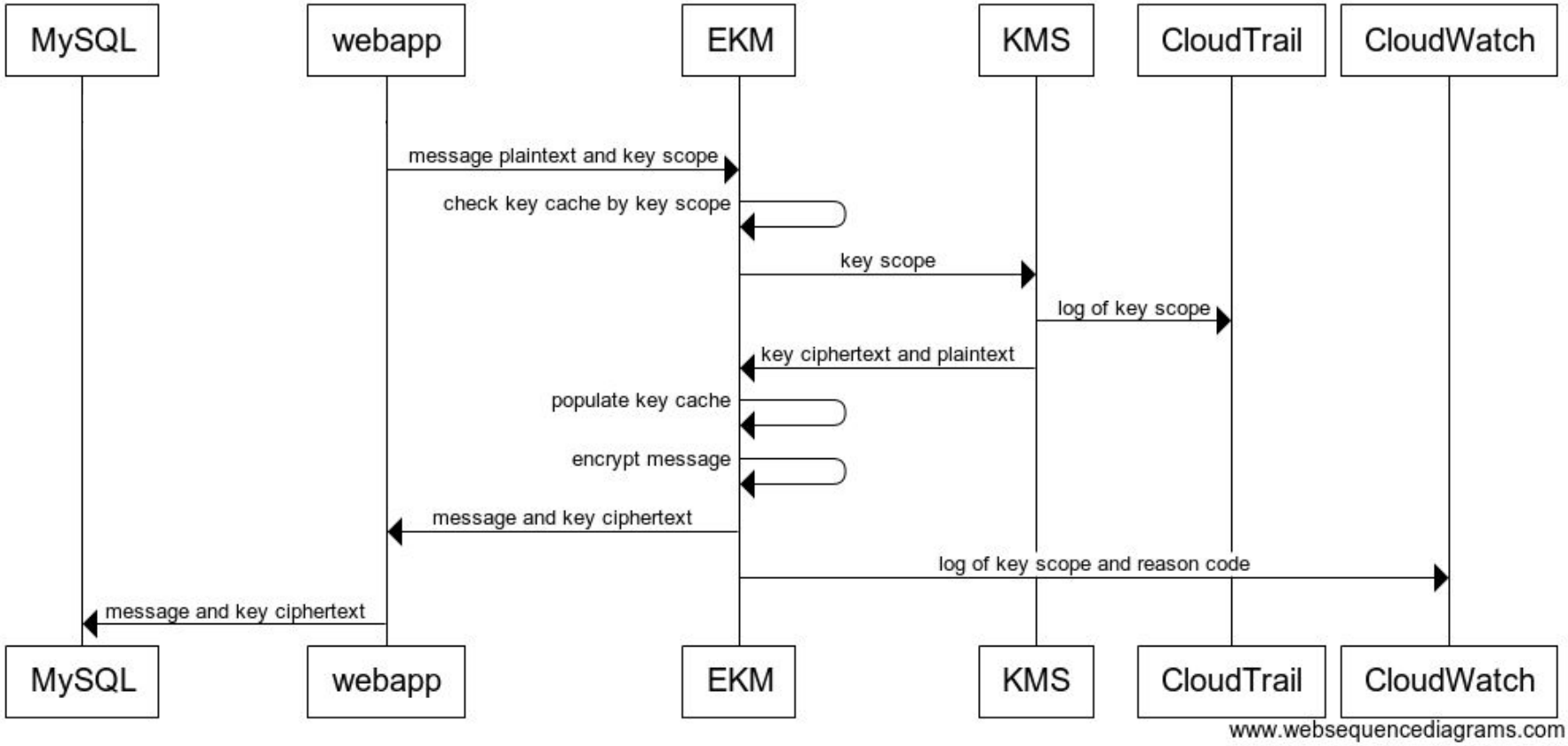
**Control** of key access by organization, workspace, channel, and time

slack

# High-level design

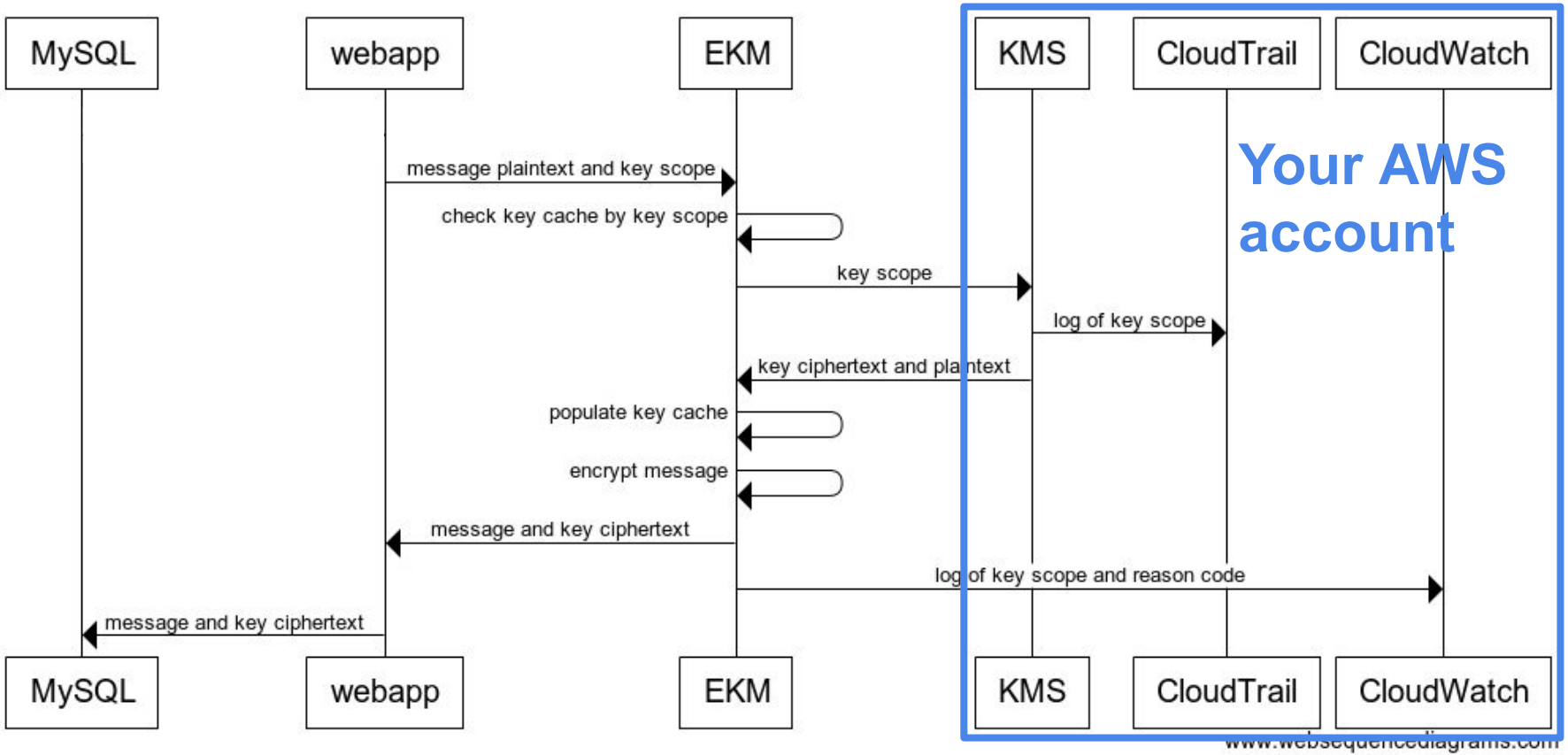
- Each time a message is sent or a file is uploaded, encrypt it and use the customer's master key to encrypt the data key
- Each time a message or file is read, use those same keys to decrypt it
- Use many data keys, each covering a small slice of messages or a single file
- Give customers a log of all access to those data keys so they know what's being decrypted
- Give customers ownership of the master key
- Cache data keys in memory for five minutes to preserve performance

# Slack EKM encryption

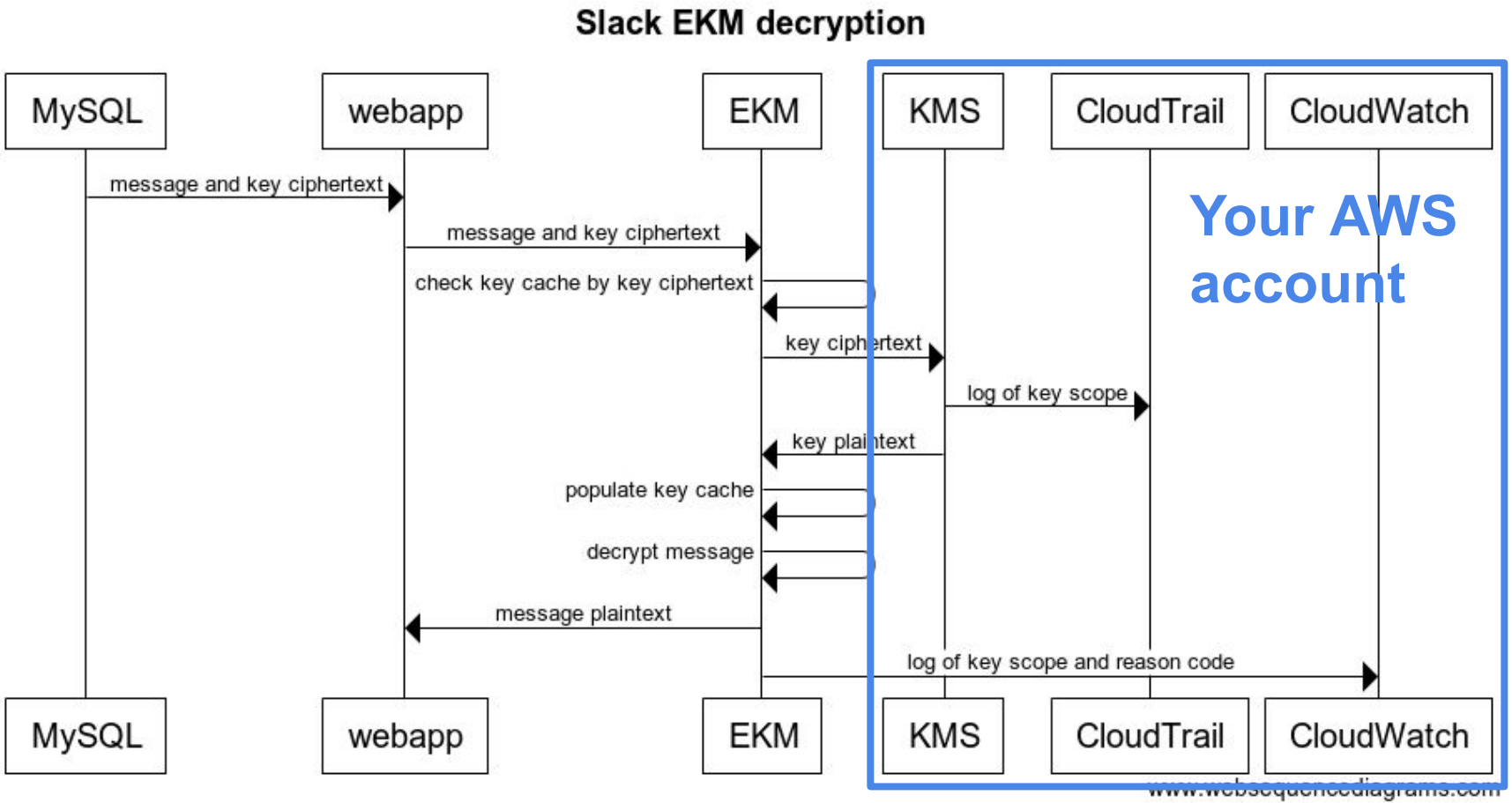



slack

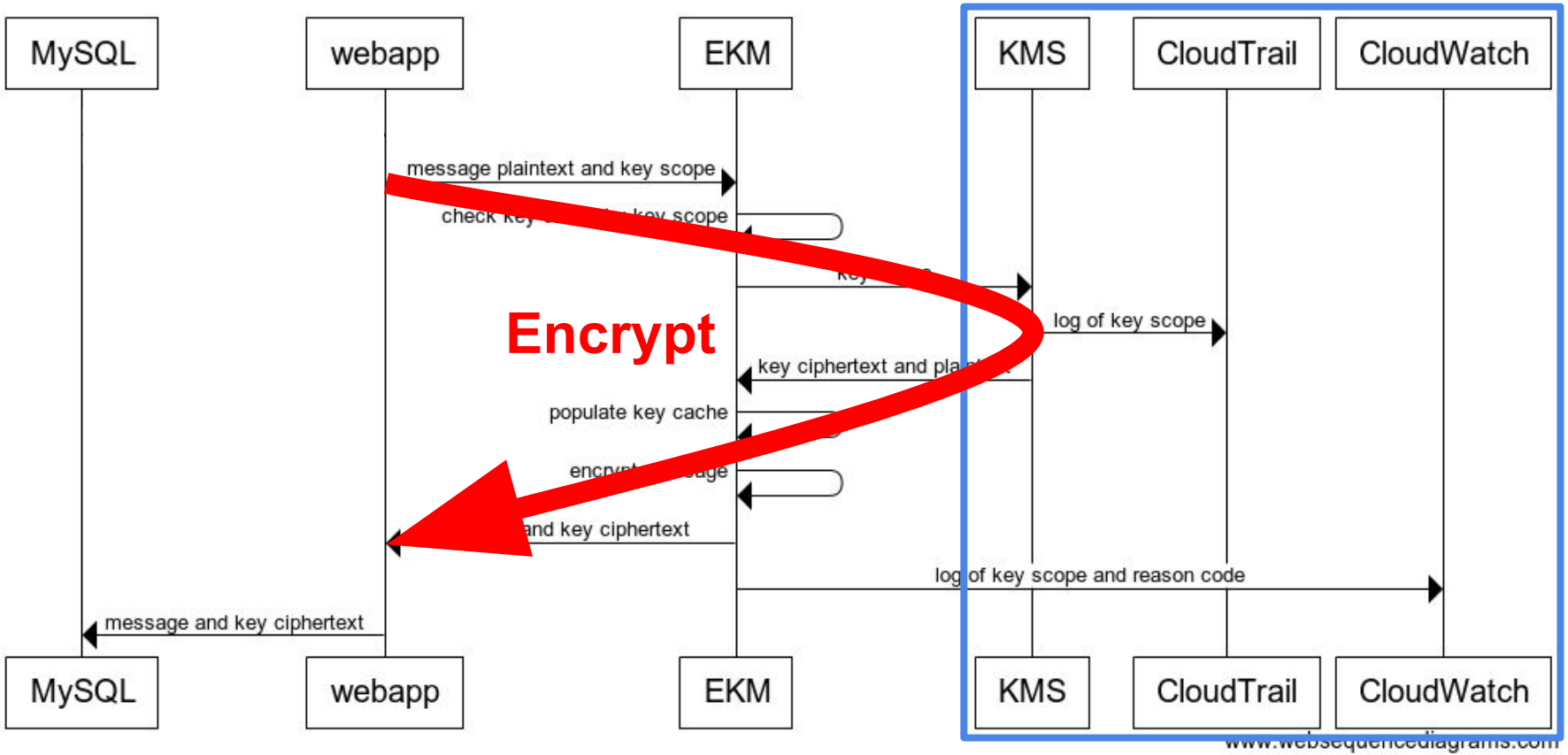
# Slack EKM encryption




slack

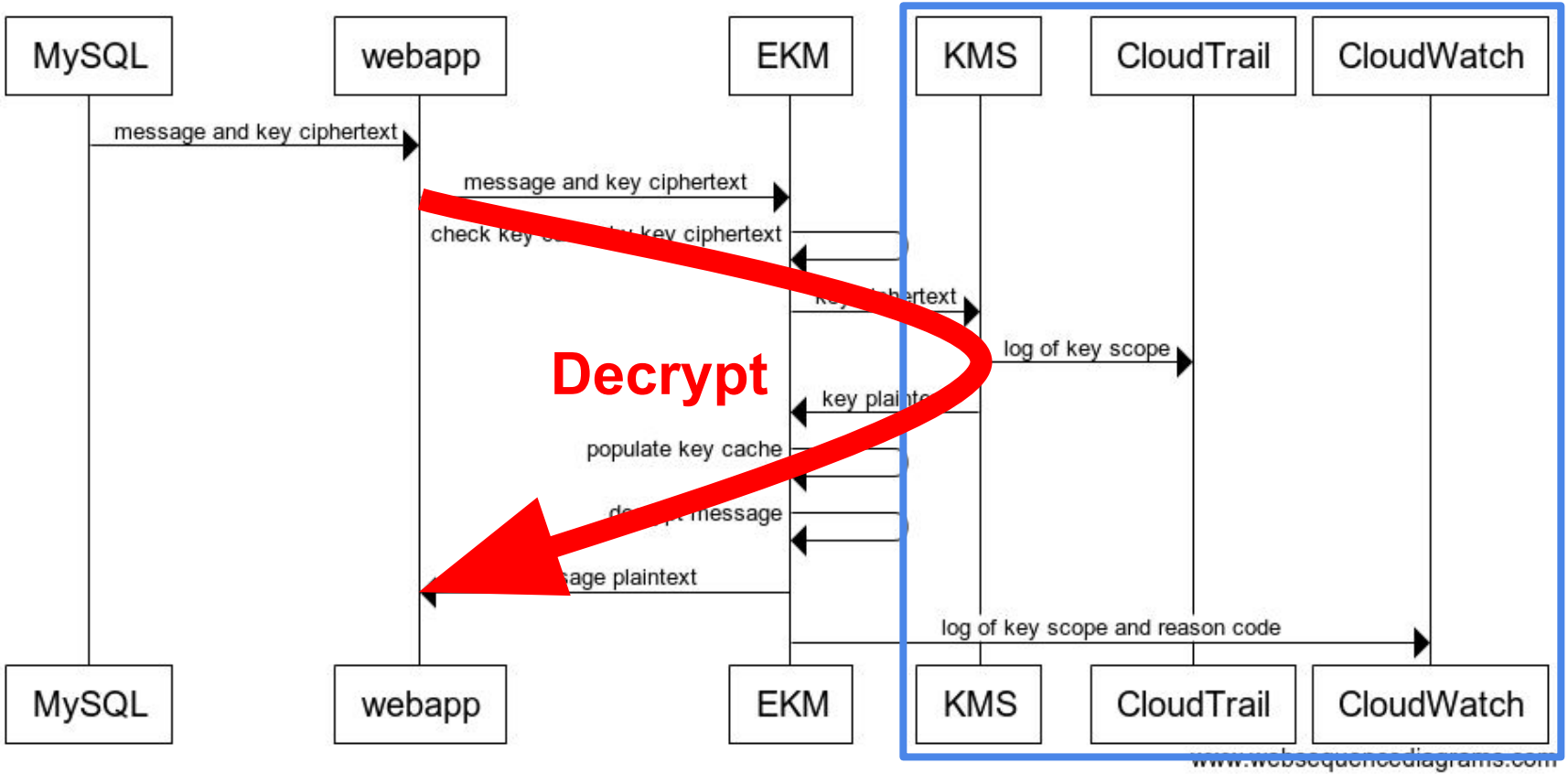

Slack EKM decryption
MySQL
webapp
EKM
KMS
CloudTrail
CloudWatch
Your AWS account
message and key ciphertext
message and key ciphertext
check key cache by key ciphertext
key ciphertext
log of key scope
key plaintext
populate key cache
decrypt message
message plaintext
log of key scope and reason code
MySQL
webapp
EKM
KMS
CloudTrail
CloudWatch

# Slack EKM encryption

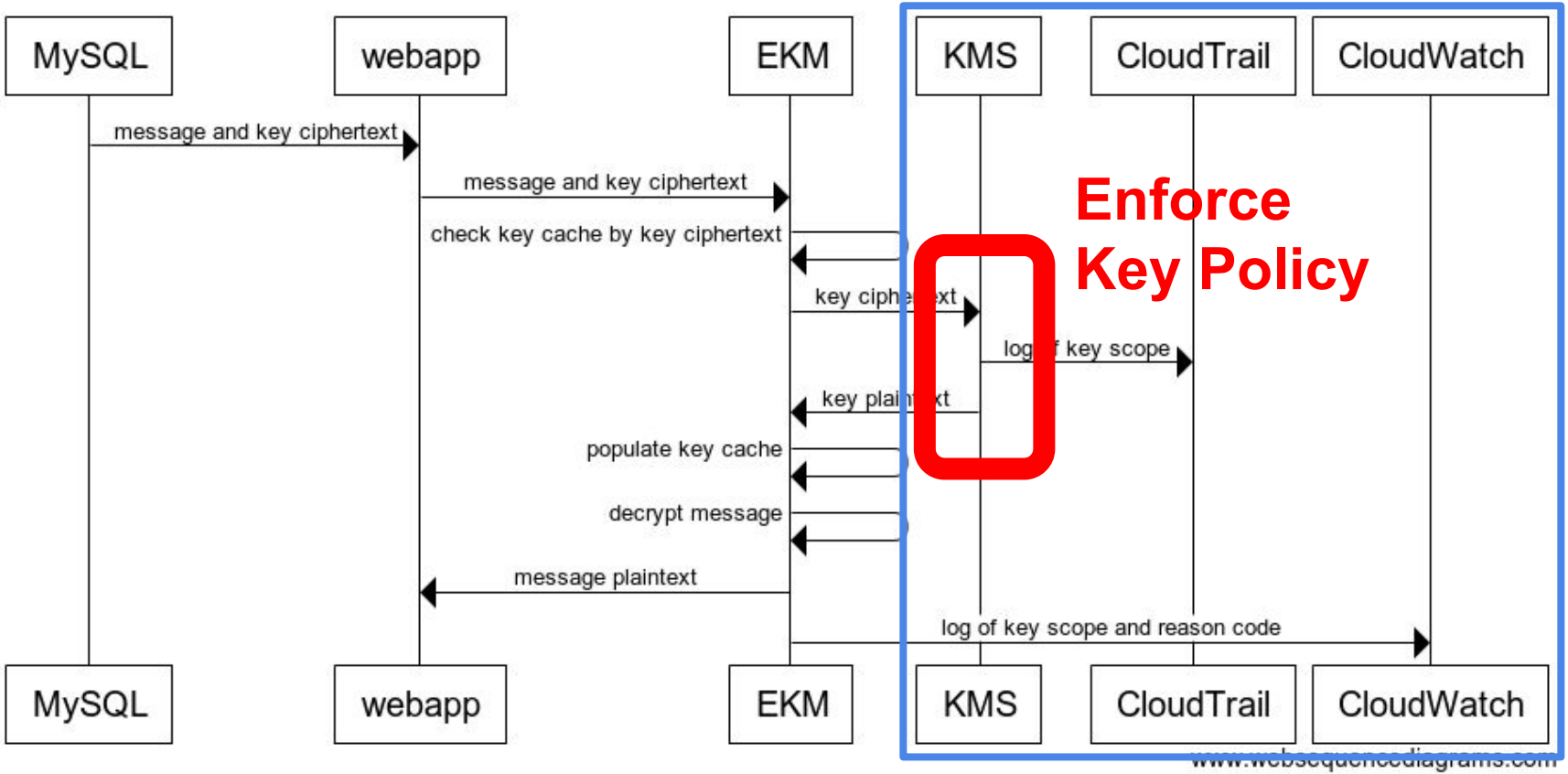



slack

# Slack EKM decryption

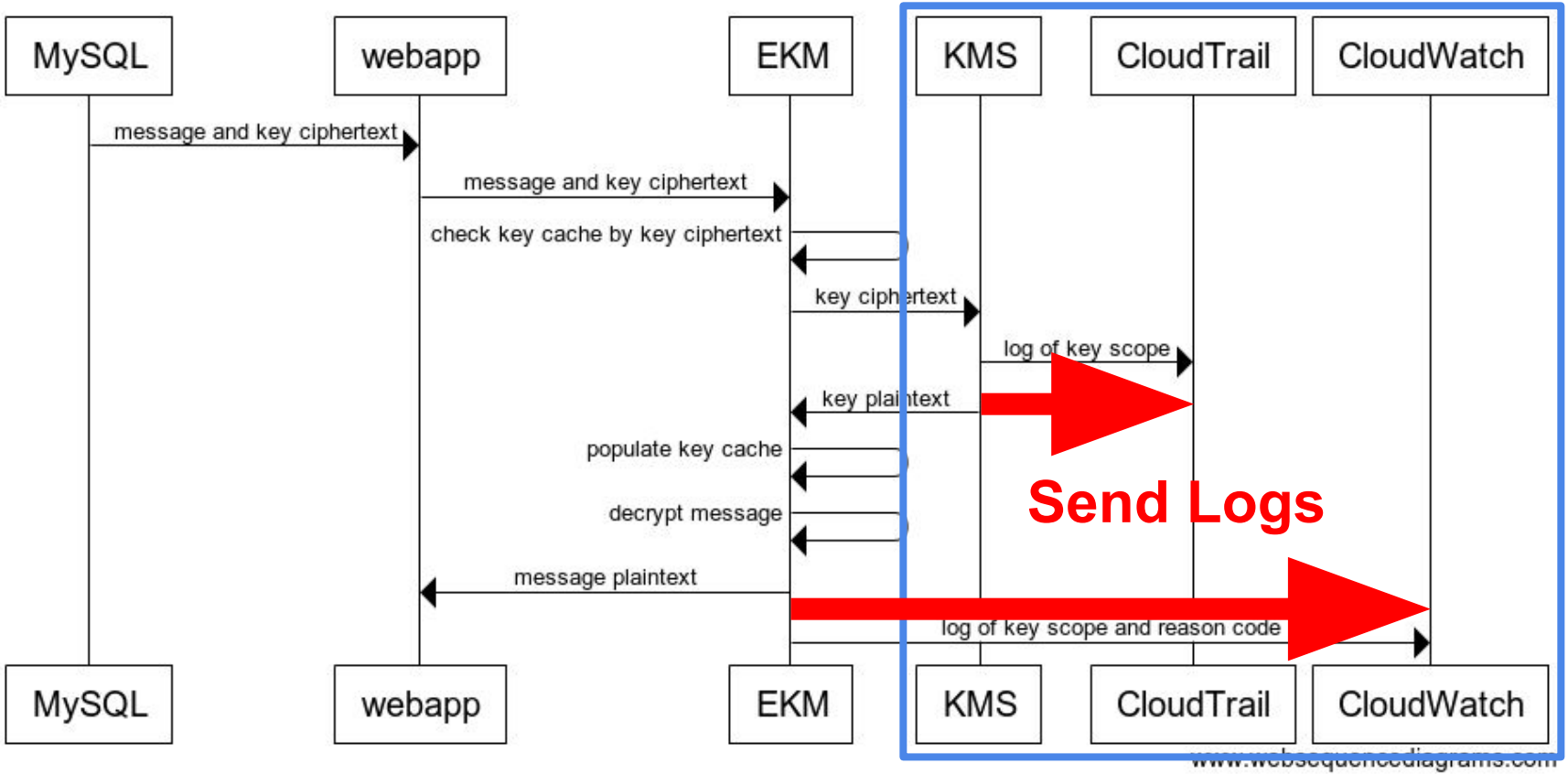


# Slack EKM decryption




slack

# Slack EKM decryption



# EncryptionContext scopes data keys to data

A message is encrypted with an encryption key that's scoped to:

- The organization that sent it
- The workspace in which the channel appears, if applicable
- The channel in which the message appears
- The hour in which the message was sent

A file is encrypted with an encryption key that's scoped to:

- The organization that sent it
- The file itself

slack

# Example logs

## CloudTrail

```
{
  "eventName": "Decrypt",
  "requestParameters": {
    "encryptionContext":{
      "C": "CD11VKXL3",
      "T": "TD2FCEBLN",
      "H": "2018-10-24T21",
      "O": "ED14RK2GJ"
    }
  },
  // ...
}
```

## CloudWatch Logs

```
{
  "Action": "Decrypt",
  "KeyScope": {
    "C": "CD11VKXL3",
    "H": "2018-10-24T21",
    "O": "ED14RK2GJ",
    "T": "TD2FCEBLN"
  },
  "Reason": "history"
}
```

slack

# Example policies:  Baseline

```
{
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::152659312504:root"},
  "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:O": "ED14RK2GJ"
    }
  }
}
```

slack

# Example policies:  Lockdown

```
{
  "Effect": "Deny",
  "Principal": {"AWS": "arn:aws:iam::152659312504:root"},
  "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:O": "ED14RK2GJ"
    }
  }
}
```

slack

# Example policies:  Lockdown for one channel

```
{
  "Effect": "Deny",
  "Principal": {"AWS": "arn:aws:iam::152659312504:root"},
  "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:C": "CD11VKXL3",
      "kms:EncryptionContext:O": "ED14RK2GJ"
    }
  }
}
```

slack

# Example policies:  Lockdown a single month

```
{
  "Effect": "Deny",
  "Principal": {"AWS": "arn:aws:iam::152659312504:root"},
  "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:O": "ED14RK2GJ"
    },
    "StringLike": {
      "kms:EncryptionContext:H": "2018-07-*"
    }
  }
}
```

slack

# Example policies: Combining channel and time

```
{
  "Effect": "Deny",
  "Principal": {"AWS": "arn:aws:iam::152659312504:root"},
  "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:C": "CD11VKXL3",
      "kms:EncryptionContext:O": "ED14RK2GJ"
    },
    "StringLike": {
      "kms:EncryptionContext:H": "2018-07-*"
    }
  }
}
```

slack

# Slack EKM

- Most importantly, when you're enrolled in EKM, **Slack remains Slack**
- You gain **control** of and **visibility** into how your encryption keys are being used
- And AWS KMS makes it fast and highly available

slack