

# 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 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

The screenshot displays a Slack workspace for 'Acme Sales' with a user profile for Tina Chen. The left sidebar shows a list of channels, with '# sales-team' selected. The main content area shows the '#sales-team' channel with a search bar and a list of messages. All messages are redacted with a lock icon and the text: 'This message can't be shown' or 'This file can't be shown', followed by a 'Learn more' link. The bottom of the interface shows a message input field with a plus icon and the text 'Message #sales-team'.

# Slack EKM to end users

The screenshot shows a Slack channel named "#sales-team" in a workspace called "Acme Sales". The channel has 90 members and a search bar. The message history includes:

- A message from Tina Chen: "Looking forward to our quarterly NPS report. I've got a good feeling about it."
- A message from Wayne Fan: "Could someone help me interpret this Zendesk ticket re: the internal dashboard?"
- A message from Sara Culver: "Might be good to get some thoughts from @Tina Chen"
- A message from Shannon Tinkley: "Zendesk Ticket Reports Now Available!"

The main message in the channel is from Tina Chen, dated 1:12 PM, with the text: "Any updates on the Tangerine deal?". This message is suspended, indicated by a lock icon and the text: "This message can't be shown. Your admins have suspended everyone's access to this content. Learn more". The input field at the bottom contains the text "Any updates on the Tangerine deal?".

The screenshot shows the same Slack channel "#sales-team" in "Acme Sales". The message history includes:

- A message from Sara Culver: "Might be good to get some thoughts from @Tina Chen"
- A message from Shannon Tinkley: "Zendesk Ticket Reports Now Available!"

The main message in the channel is from Shannon Tinkley, dated 11:49 AM, with the text: "Zendesk Ticket Reports Now Available!". The message content is:

Our customers have questions, feedback, and problems that they need solved and it's our mission to provide a predictably excellent experience for everyone interacting with Acme. Before today, it was difficult for us to aggregate the requests that they submitted to us and provide high level reports back to them. Given the nature of our systems, we need to keep policy in mind when sharing information and we needed to explore creative ways to build reports that met our requirements.

Today, I'm excited to announce that we have our first version of a **Customer Facing Zendesk Ticket Report** available for you to use, download and share with your customers!

<https://analytics.acme.com/dashboard/84012>

👍 33 ❤️ 12

4 replies Last reply today at 4:28 PM

This message can't be shown. Your admins have suspended everyone's access to this content. Learn more

Tina Chen 1:12 PM  
Any updates on the Tangerine deal?  
Your message couldn't be sent because your admins have disabled sending messages to this channel. Clear

The input field at the bottom contains the text "Message #sales-team".

# Slack EKM provides...

---

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

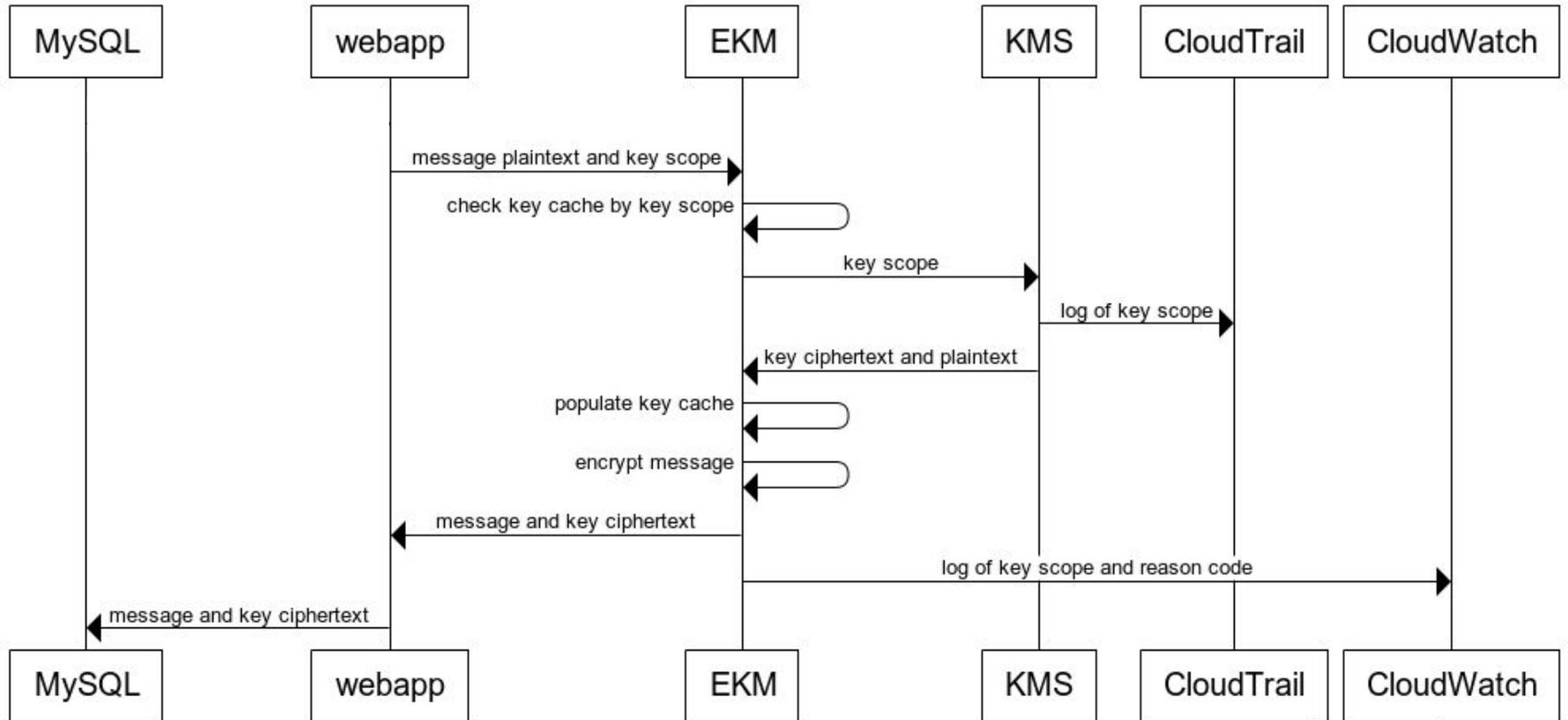
**Control** of key access by organization, workspace, channel, and time

# High-level design

---

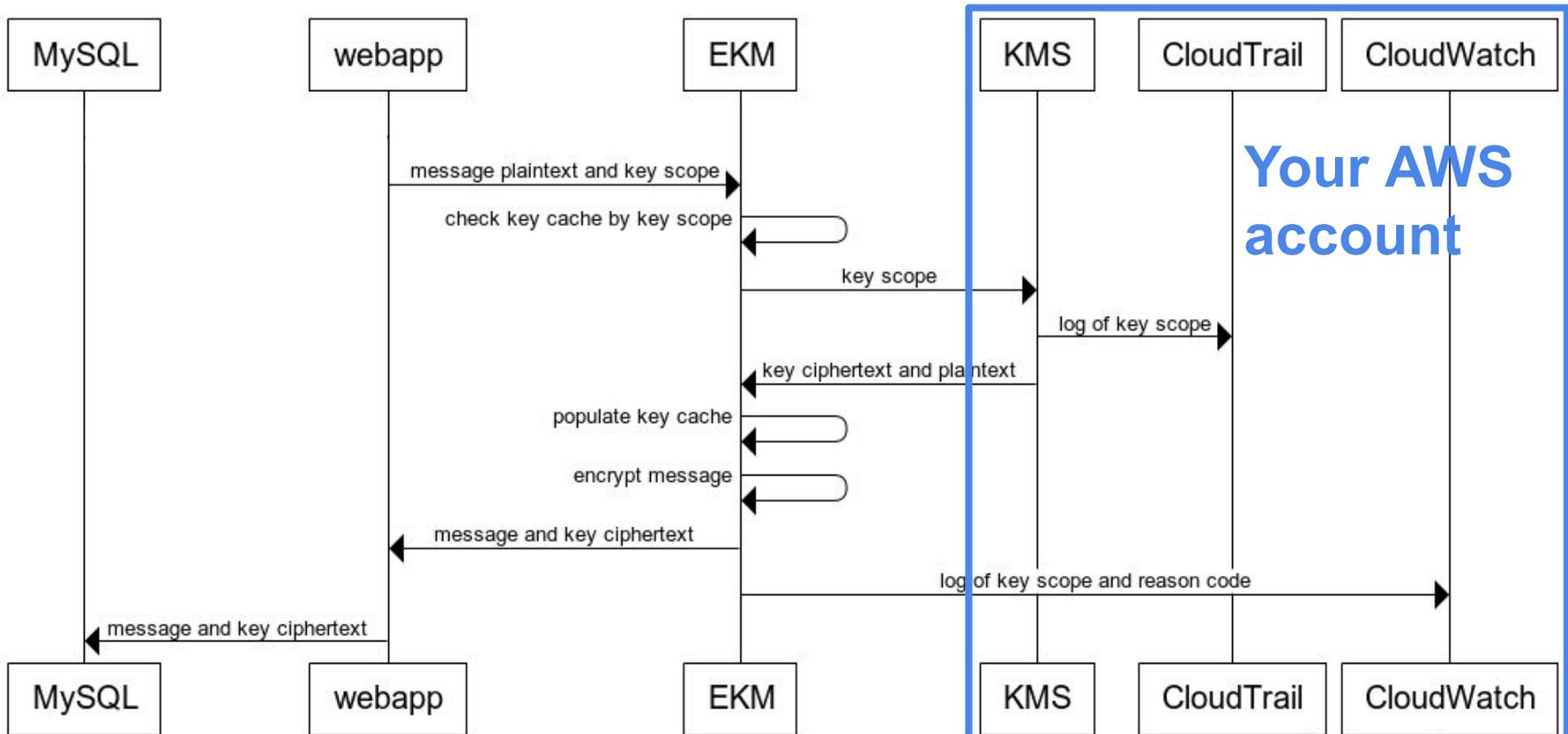
- Each time a message is sent or a file is uploaded, encrypt it and use the customer's master key to encrypt the data key
- Each time a message or file is read, use those same keys to decrypt it
- Use many data keys, each covering a small slice of messages or a single file
- Give customers a log of all 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



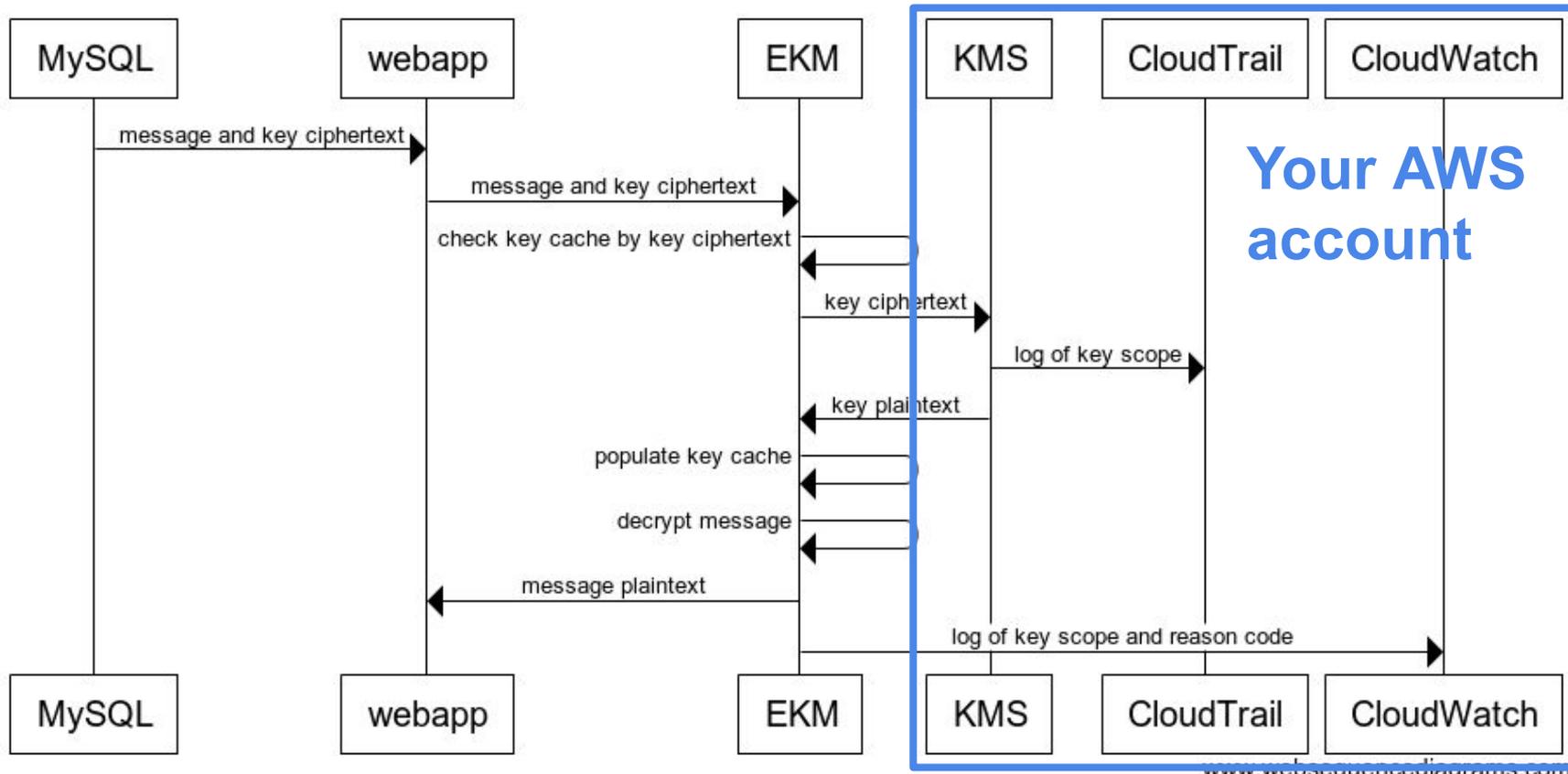
www.websequencediagrams.com

# Slack EKM encryption

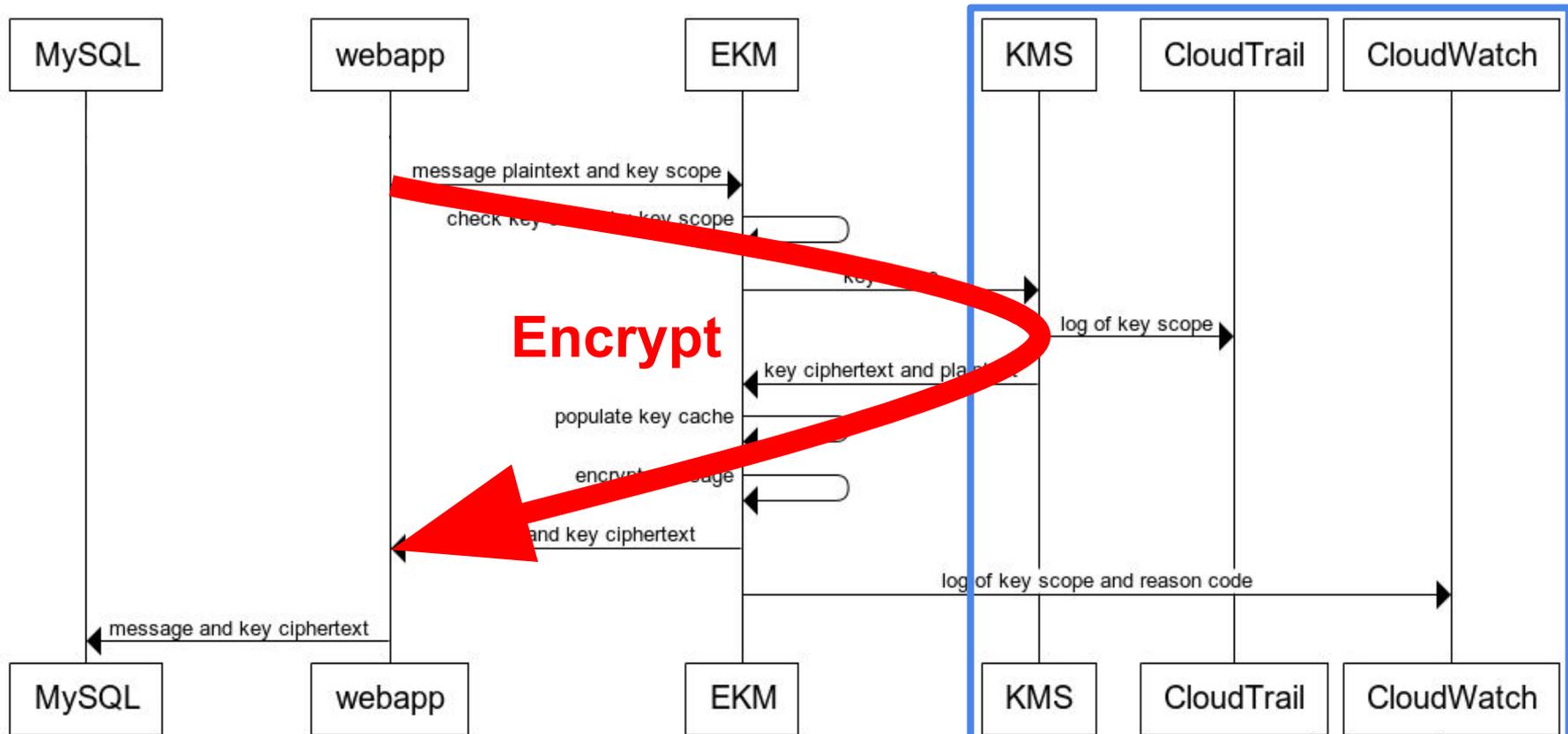


www.websequencediagrams.com

## Slack EKM decryption

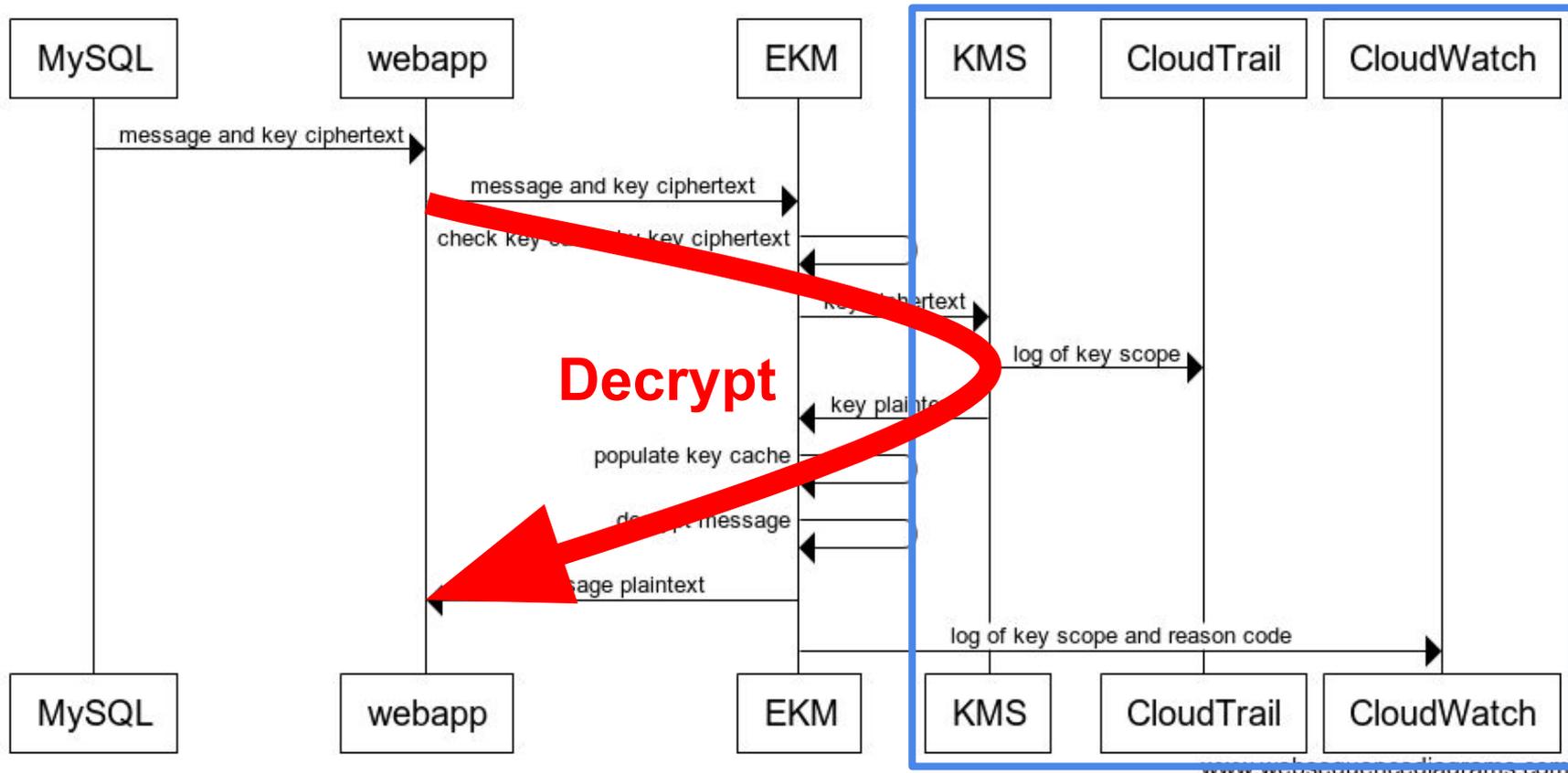


# Slack EKM encryption



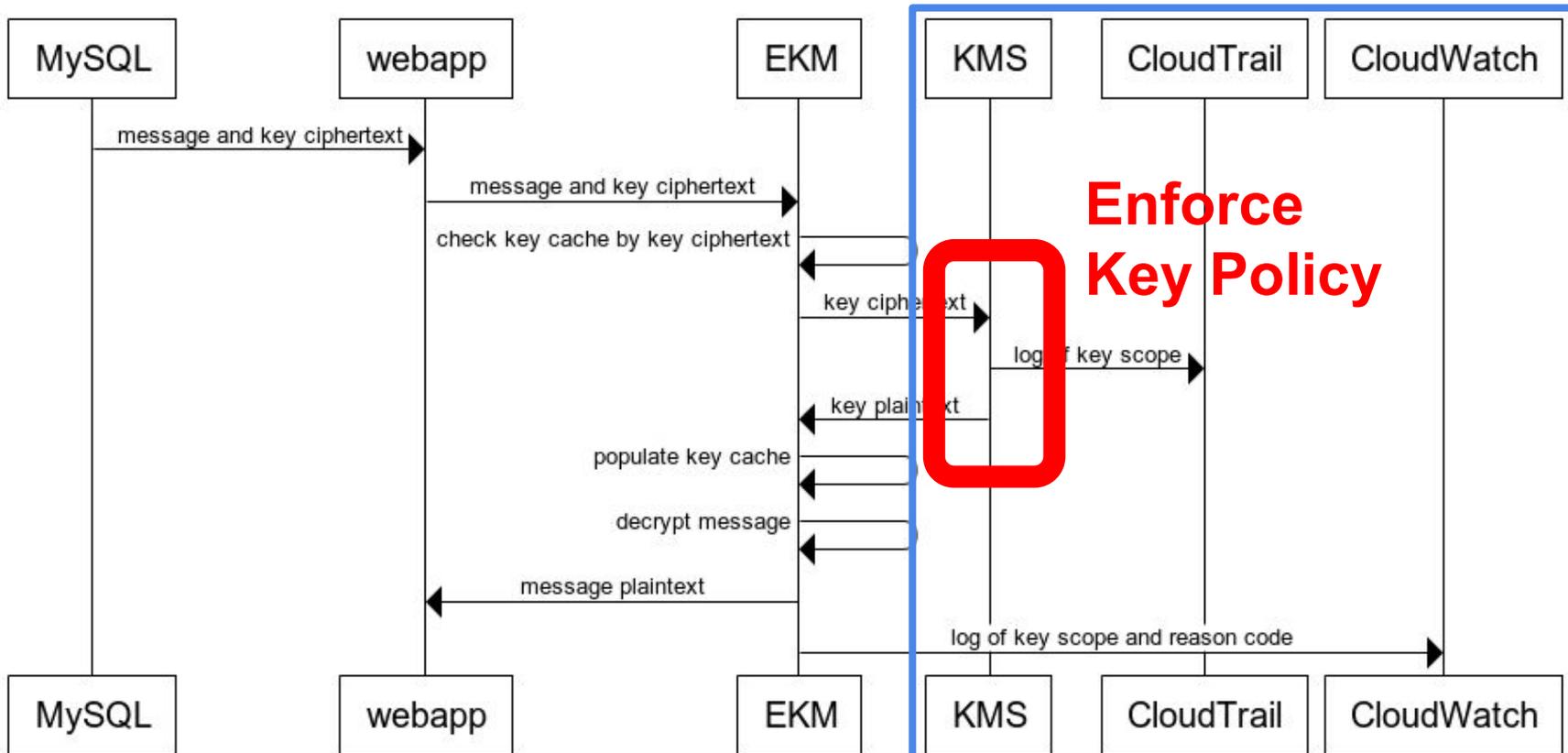
www.websequencediagrams.com

# Slack EKM decryption

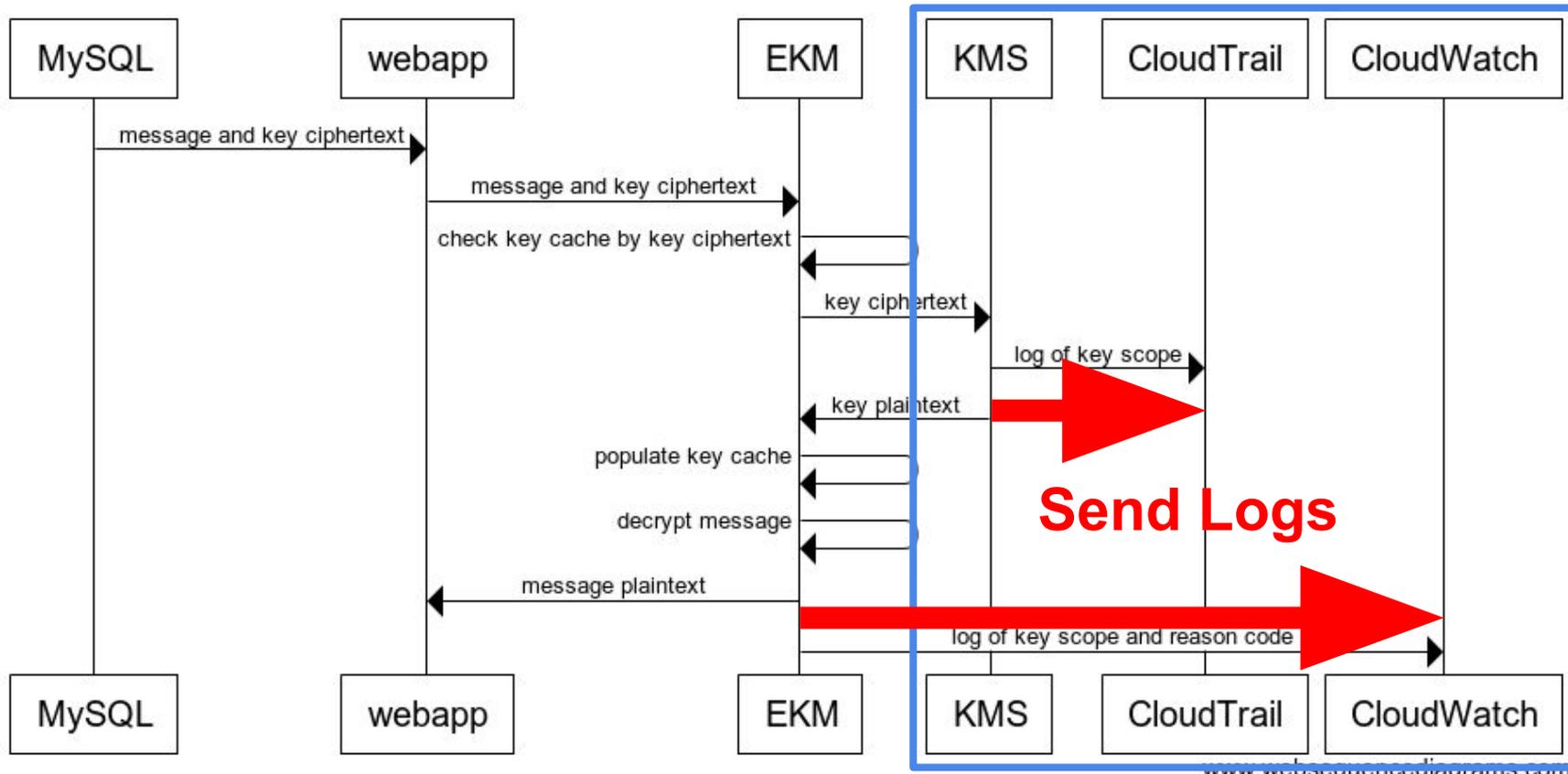


www.websequencediagrams.com

## Slack EKM decryption



## Slack EKM decryption



www.websequencediagrams.com

# 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

# 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"
}
```

# Example policies: Baseline

---

```
{
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::152659312504:root"},
  "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:0": "ED14RK2GJ"
    }
  }
}
```

# Example policies: Lockdown

---

```
{
  "Effect": "Deny",
  "Principal": {"AWS": "arn:aws:iam::152659312504:root"},
  "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:0": "ED14RK2GJ"
    }
  }
}
```

# 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"
    }
  }
}
```

# 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:0": "ED14RK2GJ"
    },
    "StringLike": {
      "kms:EncryptionContext:H": "2018-07-*"
    }
  }
}
```

# 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 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