Email Encryption

Real world solutions

Martijn Brinkers
martijn@ciphermail.com

ciphermail
email encryption

FOUNDED IN 2008

BASED IN AMSTERDAM

PRIVATELY OWNED

FOCUS:
EMAIL ENCRYPTION & DIGITAL SIGNING

FOCUS:
GATEWAY LEVEL

CUSTOMERS WORLDWIDE

ANDROID SUPPORT

OPEN SOURCE COMMUNITY EDITION

HSM SUPPORT

EASE OF USE

Take home messages

1. Internal & external email encryption is more important than ever
   (Especially for personal information [GDPR] & information which can be used for insider trading)

2. Gateway level email encryption allows you to define and enforce company policies

3. Think about how to comply to email archiving and eDiscovery regulations with respect to email encryption

4. Use an HSM to store your private keys

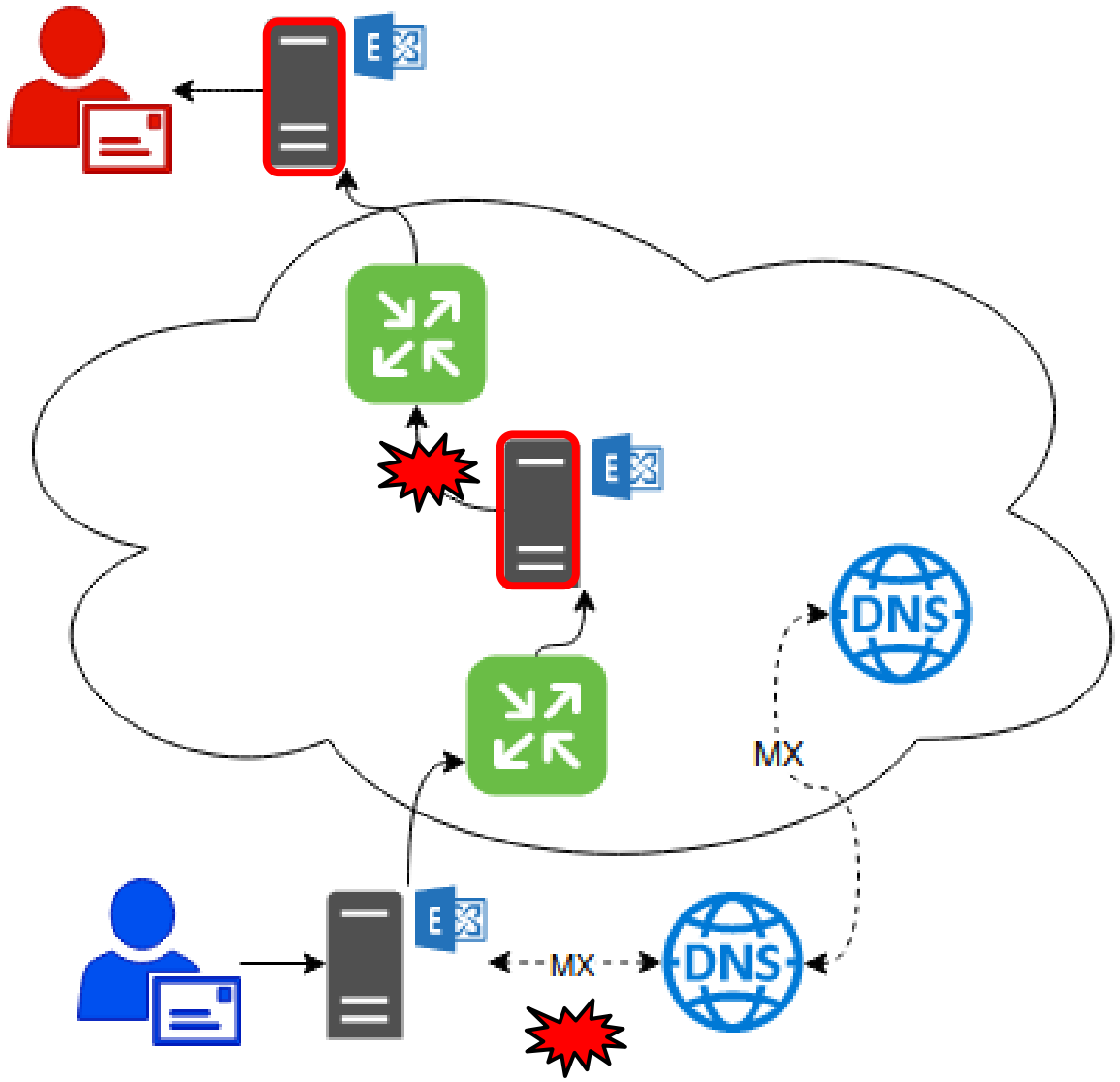
5. Email encryption is compatible with cloud-based email (O365)

Outline

1. Why we need email encryption & digital signing
2. Solution
   - Email Encryption Gateway
   - Webmail Messenger
3. Why we need internal email encryption
   - Existing solution & Challenges
4. Challenge 1: Archiving & eDiscovery
   - Explanation, Solution, & Example
5. Challenge 2: Internal & external encryption
   - Explanation & Solution
6. Take home messages

Why we need email encryption & digital signing

1. DNS cannot be fully trusted
2. Email can be intercepted
3. DNSSEC helps, but not against interception
4. Email stored on a server is not encrypted
5. SSL/TLS only protects the channel, not the message
6. Recipient cannot check the sender

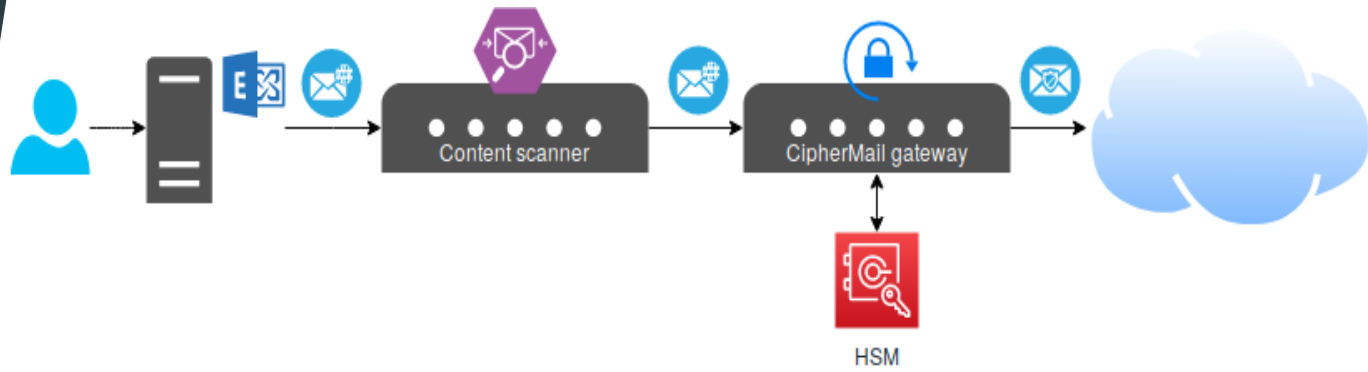


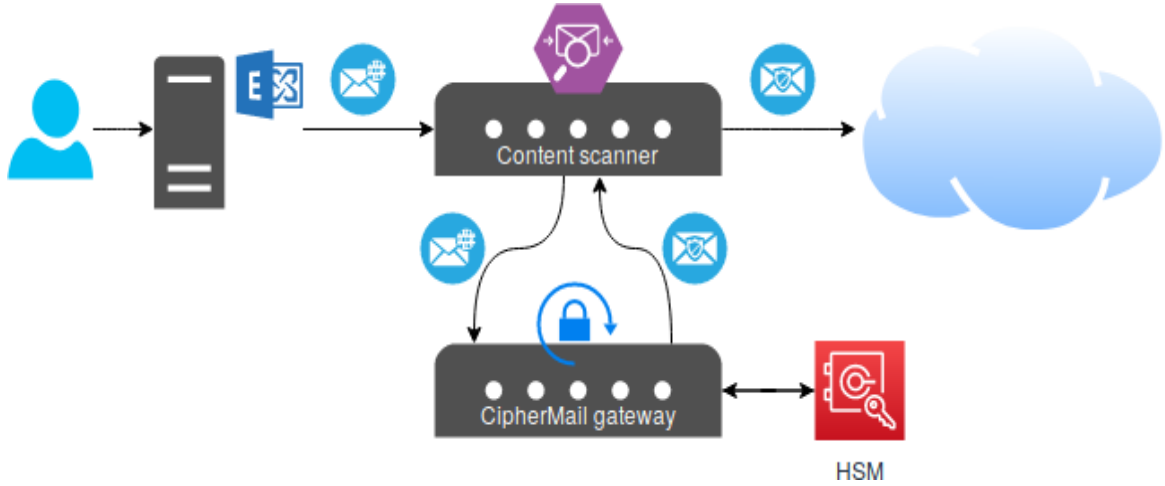
Solution
Email Encryption Gateway

- SMTP email server (MTA), Web GUI
- Supports S/MIME, PGP, PDF encryption, SSL/TLS
- Domain to domain encryption (S/MIME, PGP)
- Master/Master HA cluster
- Support for Hardware Security Modules (nCipher, Safenet, Utimaco, Securosys)
- Auto request end-user certs using built-in CA or external CA (EJBCA, GlobalSign EPKI etc.)
- DLP (quarantine, block, force encryption)
- Packages for Ubuntu, Debian, RedHat/CentOS, SUSE
- Virtual Appliance for Vmware & HyperV
- & more… (see www.ciphermail.com)

Solution
Email Encryption Gateway

- SMTP store and forward server
- Content scanning after encryption/decryption
- External email encryption

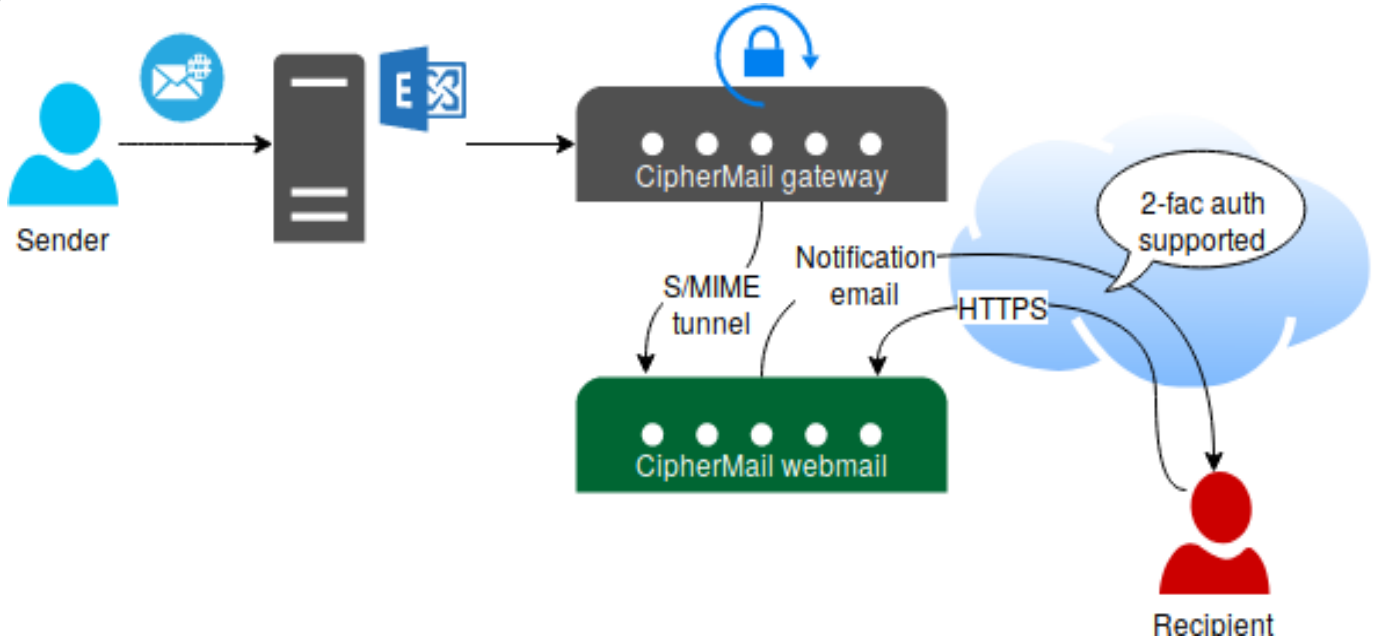




ciphermail

Solution
Webmail Messenger

- Webmail messenger is a webmail pull add-on to the gateway
- The recipient only needs a browser
- On premise
- Support for 2-factor authentication using SMS or secure token (for example Google Authenticator)
- Read confirmation can be sent back to sender after the recipient has opened the email



Why we need internal email encryption

Binnenland

De Telegraaf

Agenten gluren in pikant dossier Van Persie

door Jolande van der Graaf

ROTTERDAM - Meer dan tweehonderd Rotterdamse politieagenten hebben stiekem geprobeerd in te loggen in het afgeschermde, digitale onderzoeksdossier naar de vermeende verkrachting van de voormalige escortdame Sandra K. door voetballer Robin van Persie.

Het legertje glurende agenten had in het pikante dossier helemaal niets te zoeken, omdat het merendeel niet bij het onderzoek naar de zedenzaak betrokken was.

Robin van Persie.

De dienders hebben tegenover de commissie integriteit

Microsoft: Hackers compromised support agent's credentials to access customer email accounts

Ingrid Lunden Zack Whittaker
2 months

On the heels of a trove of 773 million emails, and tens of millions of passwords, from a variety of domains getting leaked in January, Microsoft has faced another breach affecting its web-based email services.

Microsoft has confirmed to TechCrunch that a certain "limited" number of people

Sign in
Contribute
The Guardian
News Opinion Sport Culture Lifestyle
World UK Science Cities More

Facebook

This article is more than **3 months old**

Confidential emails sent by Facebook executives leaked online

Communications between senior figures, including Mark Zuckerberg, shed new light on data use

tweakers
Zoek naar nieuws
hosted by TRUE

Tientallen medewerkers Haags ziekenhuis bekeken medisch dossier van bn'er

Tientallen medewerkers van het HagaZiekenhuis in Den Haag hebben het elektronisch patiëntendossier van een bn'er ingezien, terwijl ze niet betrokken waren bij de behandeling van die patiënt. Dat meldt EenVandaag. Het ziekenhuis heeft de zaak in onderzoek.

Het is onbekend waarom de medewerkers van het ziekenhuis het dossier in het computersysteem hebben opgevraagd, maar dat is in elk geval tegen de regels, schrijft EenVandaag. De patiënt is op de hoogte gebracht van de schending van haar privacy. Het is onbekend wanneer het ziekenhuis het onderzoek naar de zaak af heeft. Ook is onduidelijk of het ziekenhuis waarborgen in het systeem gaat aanbrengen om ongeoorloofde toegang tot medische dossiers in de toekomst te voorkomen.

USNews CIVIC

Inside Story: How Russians Hacked the Democrats' Emails

How did Russian hackers pry into Clinton campaign emails? Huge effort made quick work.

Nov. 4, 2017

FILE - In this Saturday, July 30, 2016 file photo, Democratic presidential candidate Hillary Clinton pauses while speaking at a rally in Pittsburgh during a bus tour through the rust belt. In 2016, after repeated attempts to break into various staffers' hillaryclinton.com email accounts, the hacking group known as Fancy Bear took a new tack, targeting top Clinton lieutenants at their personal Gmail addresses. (AP Photo/Andrew Harnik) THE ASSOCIATED PRESS

Three Chinese Hackers Fined $9 Million for Stealing Trade Secrets

May 11, 2017 Wang Wei

Hackers won't be spared.

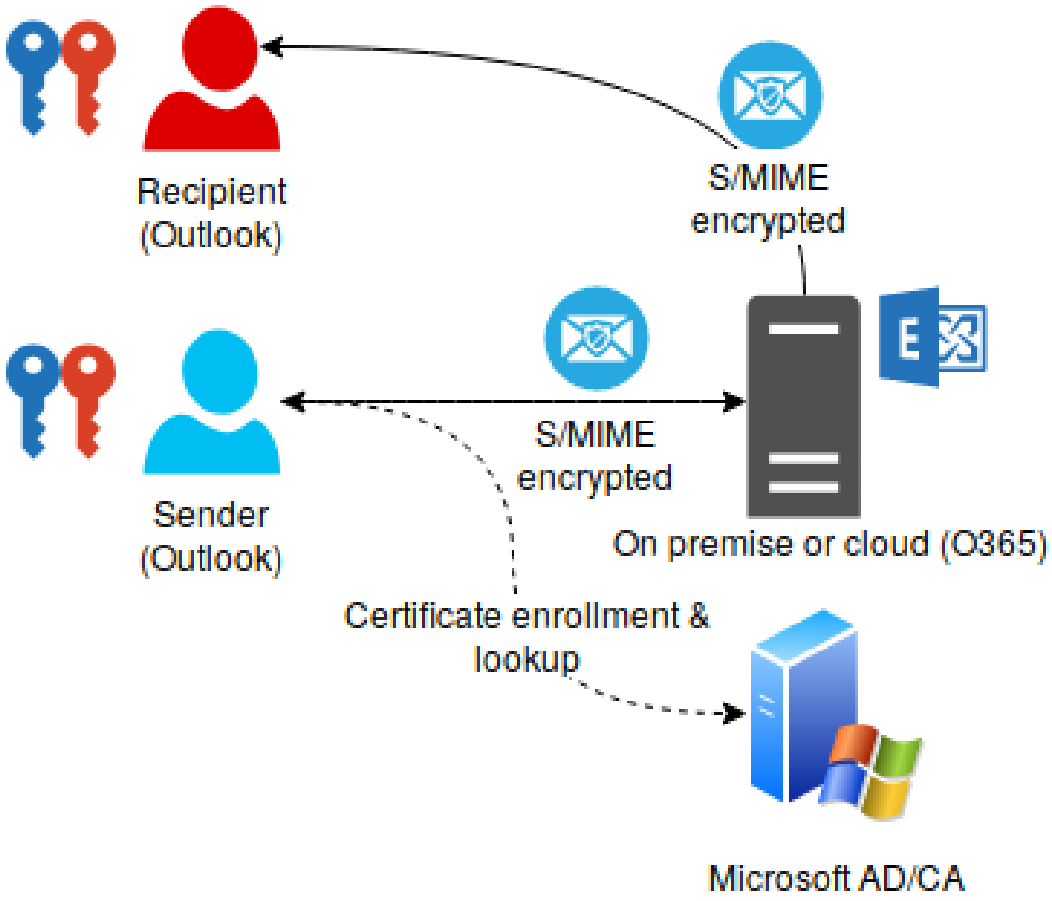
Three Chinese hackers have been ordered to pay $8.8 million (£6.8 million) after hacking email servers of two major New York-based law firms to steal corporate merger plans in December 2016 and used them to trade stocks.

The U.S. District Judge Valerie Caproni in Manhattan sued 26-year-old Iat Hong, 30-year-old Bo Zheng, and 50-year-old Hung Chin, over a multi-million dollar insider trading scam.

ciphermail

Existing solution

- "Easy" to setup with Exchange, Outlook & Microsoft CA
- S/MIME based
- Auto certificate enrollment
- Nearly painless for sending encrypted email to internal recipients



Challenges with existing solution

Two main challenges

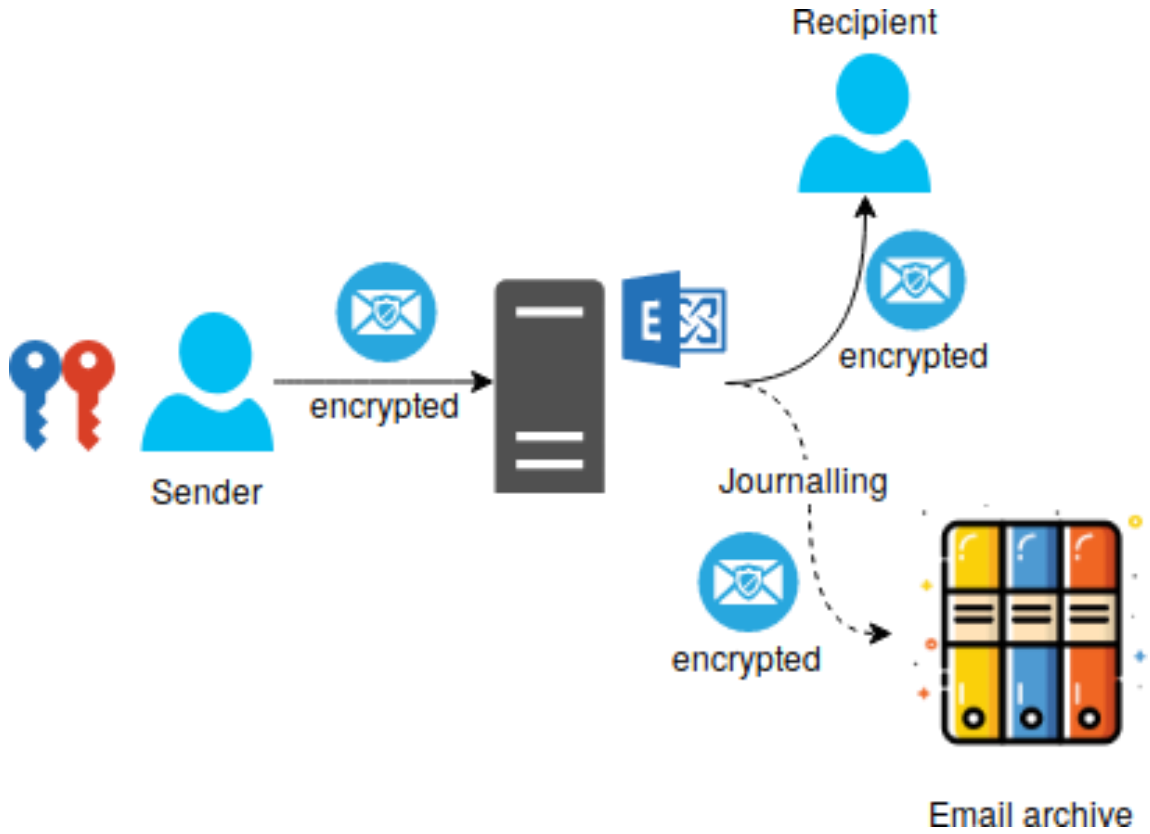
1. Email archiving & eDiscovery of encrypted email

2. Email encryption for internal & external recipients

Challenge 1: Archiving & eDiscovery

Explanation

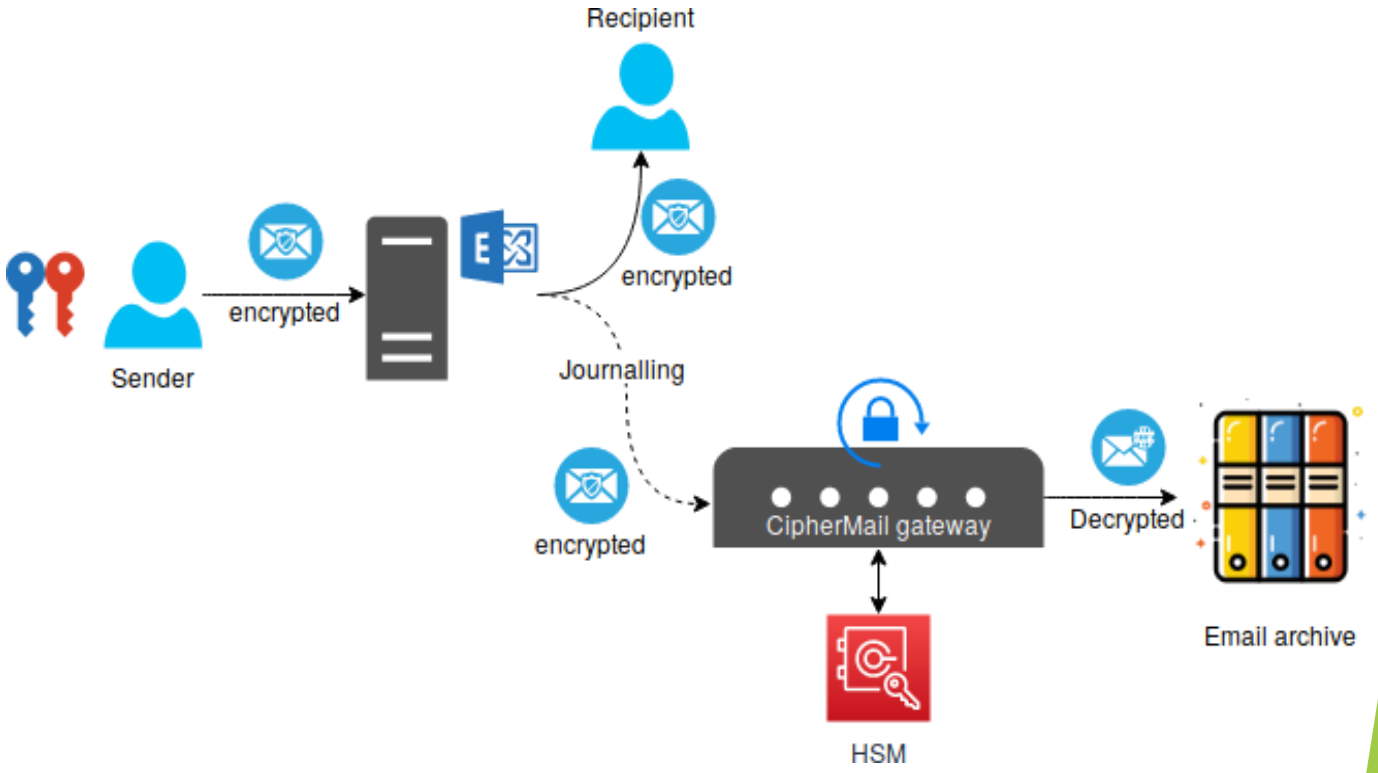
- Email encrypted by mail client = default archived in encrypted form
- eDiscovery only works if email is readable
- Archiving software must support reading encrypted email
- Regulations require email to be stored for years
- This requires that all private keys are backed up for years
- Are you 100% certain you have a copy of all keys?



Challenge 1: Archiving & eDiscovery

Solution

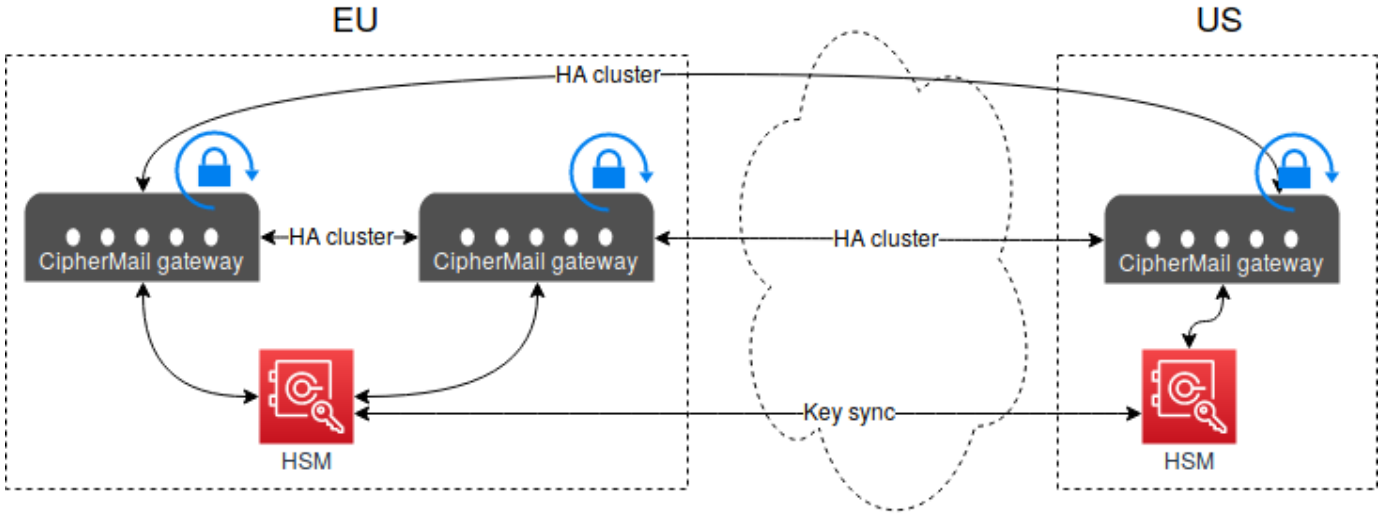
- Decrypt before archiving
- eDiscovery now possible
- Emails which cannot be decrypted are queued for investigation
- Keys can be "pushed" or "pulled“
- Keys should be stored on an HSM
- The email archiving solution should encrypt with an archiving key



Challenge 1: Archiving & eDiscovery

Example

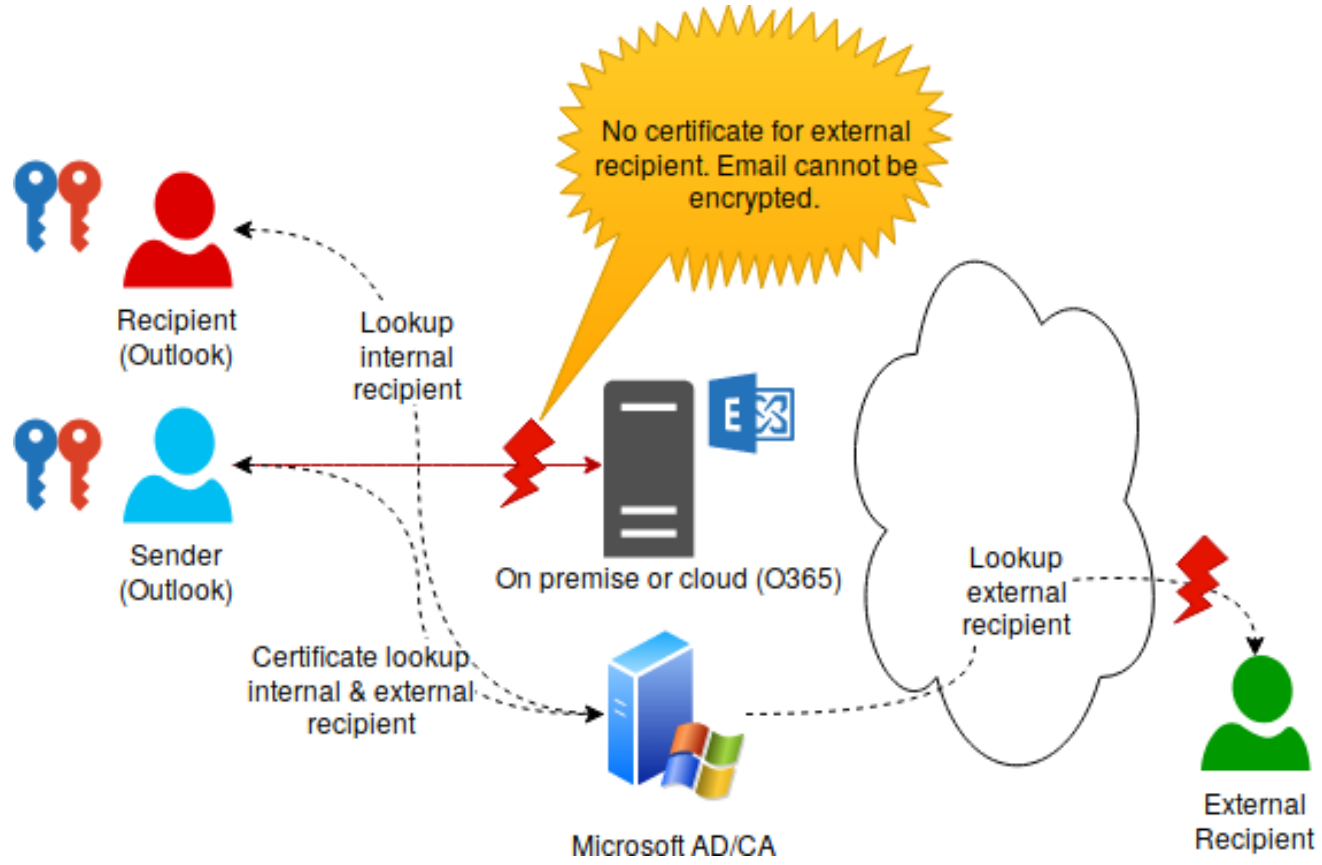
Global investment management firm with offices in over 20 locations worldwide



Challenge 2: Encryption for internal & external recipients

Explanation

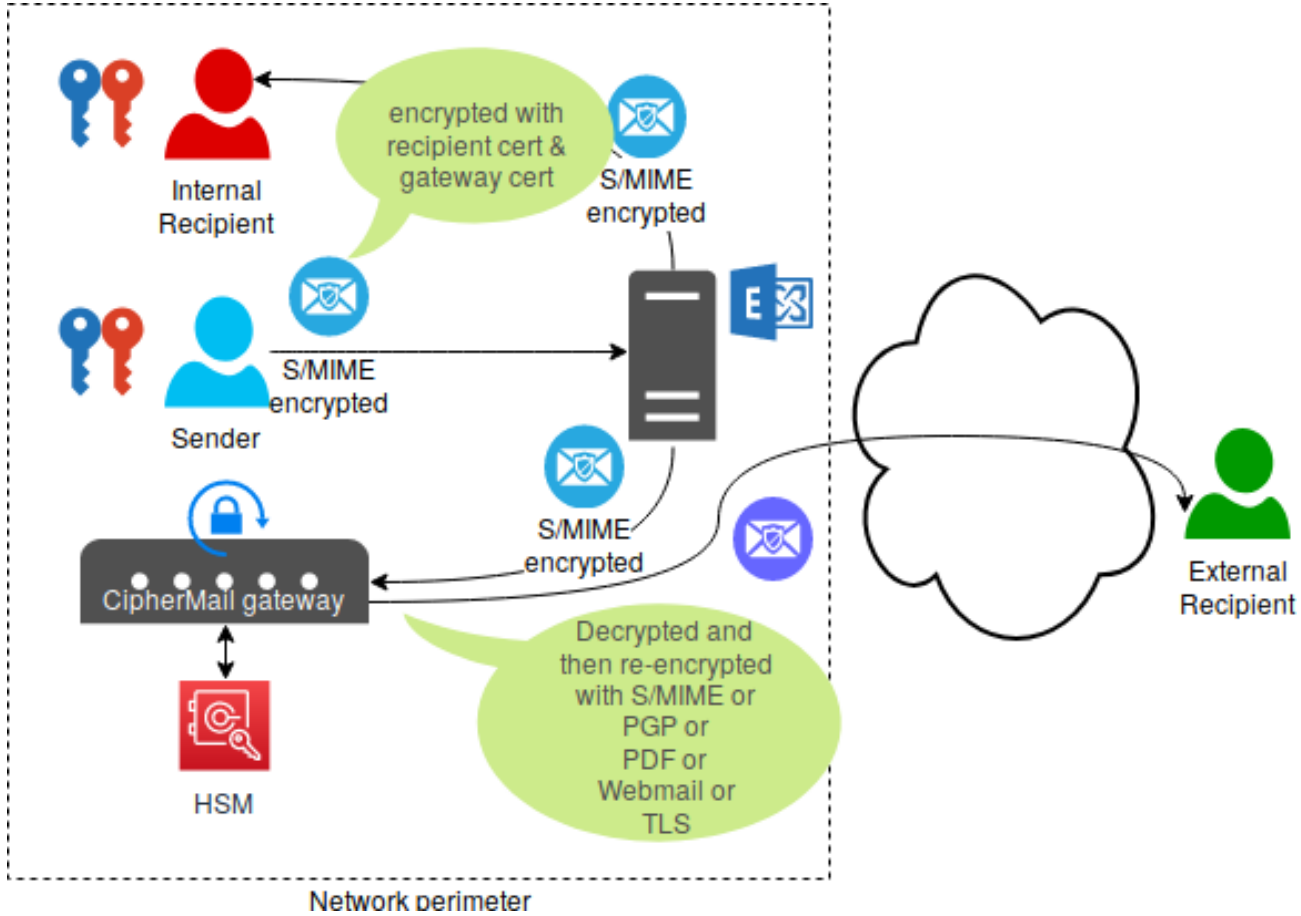
- What to do if an external recipient does not have a valid certificate?
- Or does not support S/MIME?



Challenge 2: Encryption for internal & external recipients

Solution

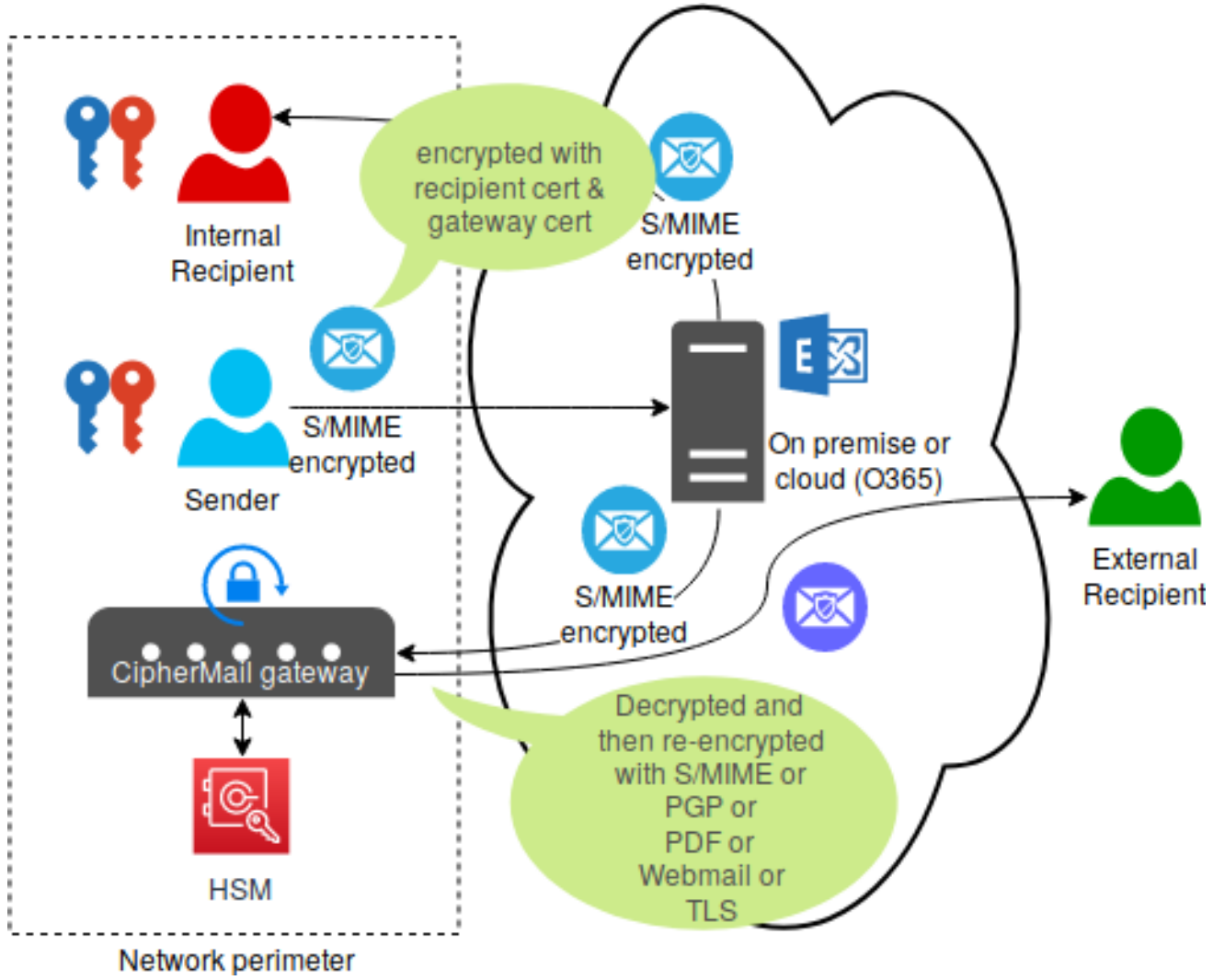
- Email for external recipients is encrypted with the gateway certificate.
- The gateway will then re-encrypt the email.



Challenge 2: Encryption for internal & external recipients

Solution

- Email encryption O365
- Microsoft manages your email (backups, login etc.)
- Encryption/Decryption is managed by the organisation (Bring Your Own Key)



Take home messages

1. Internal & external email encryption is more important than ever
   (Especially for personal information [GDPR] & information which can be used for insider trading)

2. Gateway level email encryption allows you to define and enforce company policies

3. Think about how to comply to email archiving and eDiscovery regulations with respect to email encryption

4. Use an HSM to store your private keys

5. Email encryption is compatible with cloud-based email (O365)

Thank you

Martijn Brinkers
martijn@ciphermail.com