

TeleTrust-EBCA "PKI-Workshop" 2024

Berlin, 10.10.2024

"S/MIME and Intune MDM: The Vogon Poetry of E-Mail Encryption"

Stephan Mößler, E.ON Digital Technology

TeleTrust – EBCA PKI Workshop

S/MIME and Intune MDM

A vagon poetry of mail encryption?!?

Who I'am

Stephan Mößler

Solution Architect

Cyber Security

M +491623343638

stephan.moessler@eon.com

e-on



What is a Vogon poetry?

Vogon poetry

- Hitchhiker's Guide to the Galaxy, Douglas Adams, 1979
 - Considered the third worst poetry in the universe
 - Characterized by nonsensical language
 - Used by Vogons to torture others
 - Reflects the unpleasant nature of Vogon culture

Scenario

- S/MIME is used for e-mail encryption
- Users should be able to read encrypted mails on mobile devices
- Sensitivity labels via Microsoft Information Protection (MIP)
 - Outlook Mobile must be used on client side
- Exchange servers are operated by Microsoft

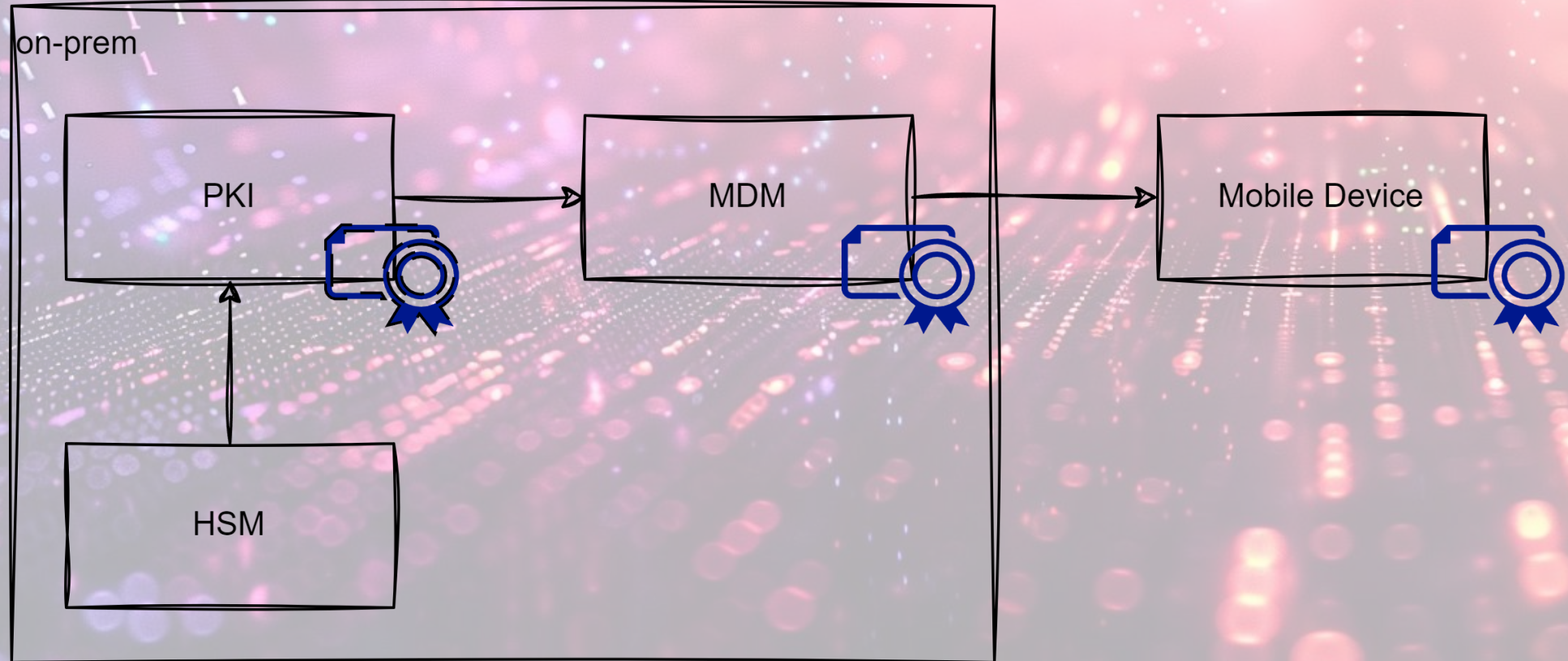
Requirements

- Encryption keys should never be exposed to Microsoft
- OS native mail client (iOS / Android) and Outlook mobile must be supported
- Solution must be automated and user friendly
- Secure cipher suites must be used

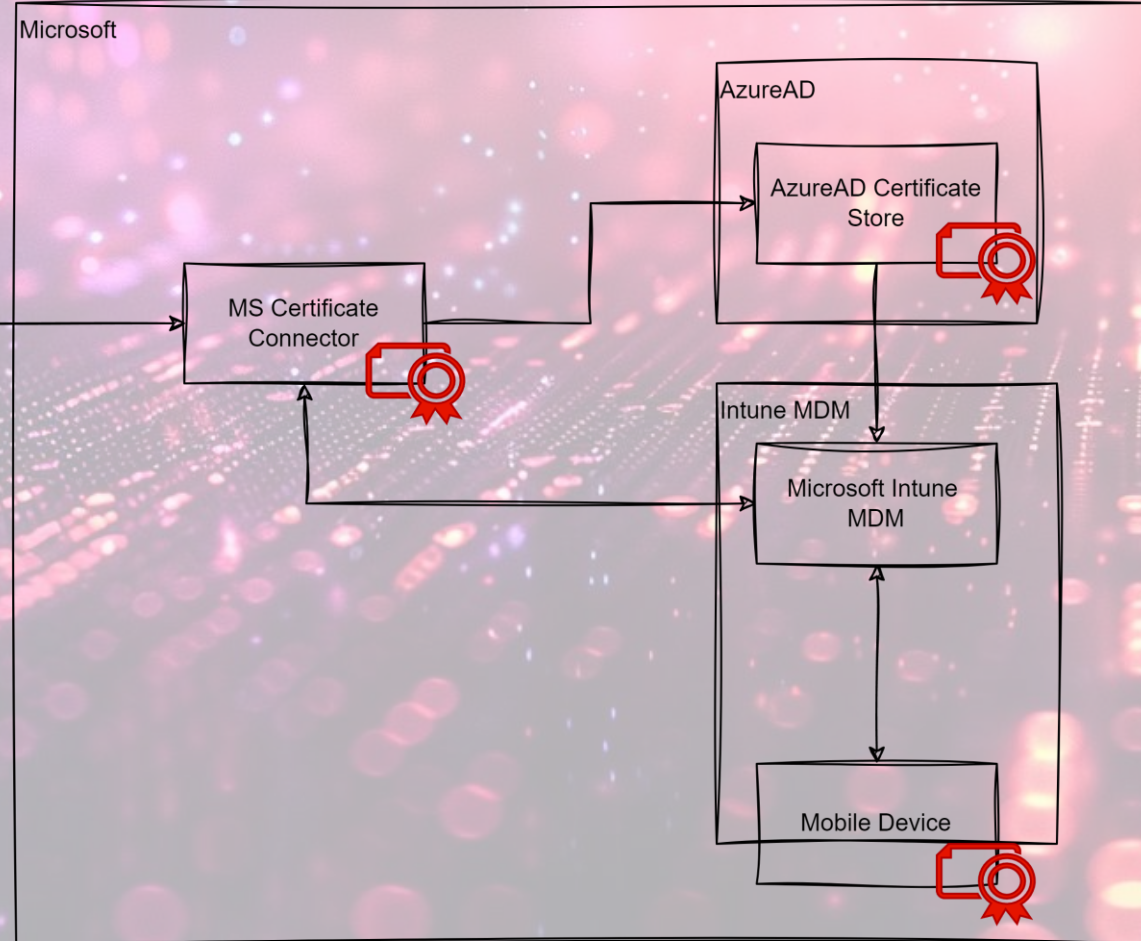
„S/MIME is only used by germans“

Microsoft PG MIP / Outlook, 2023

Architecture



MS Ref - Architecture

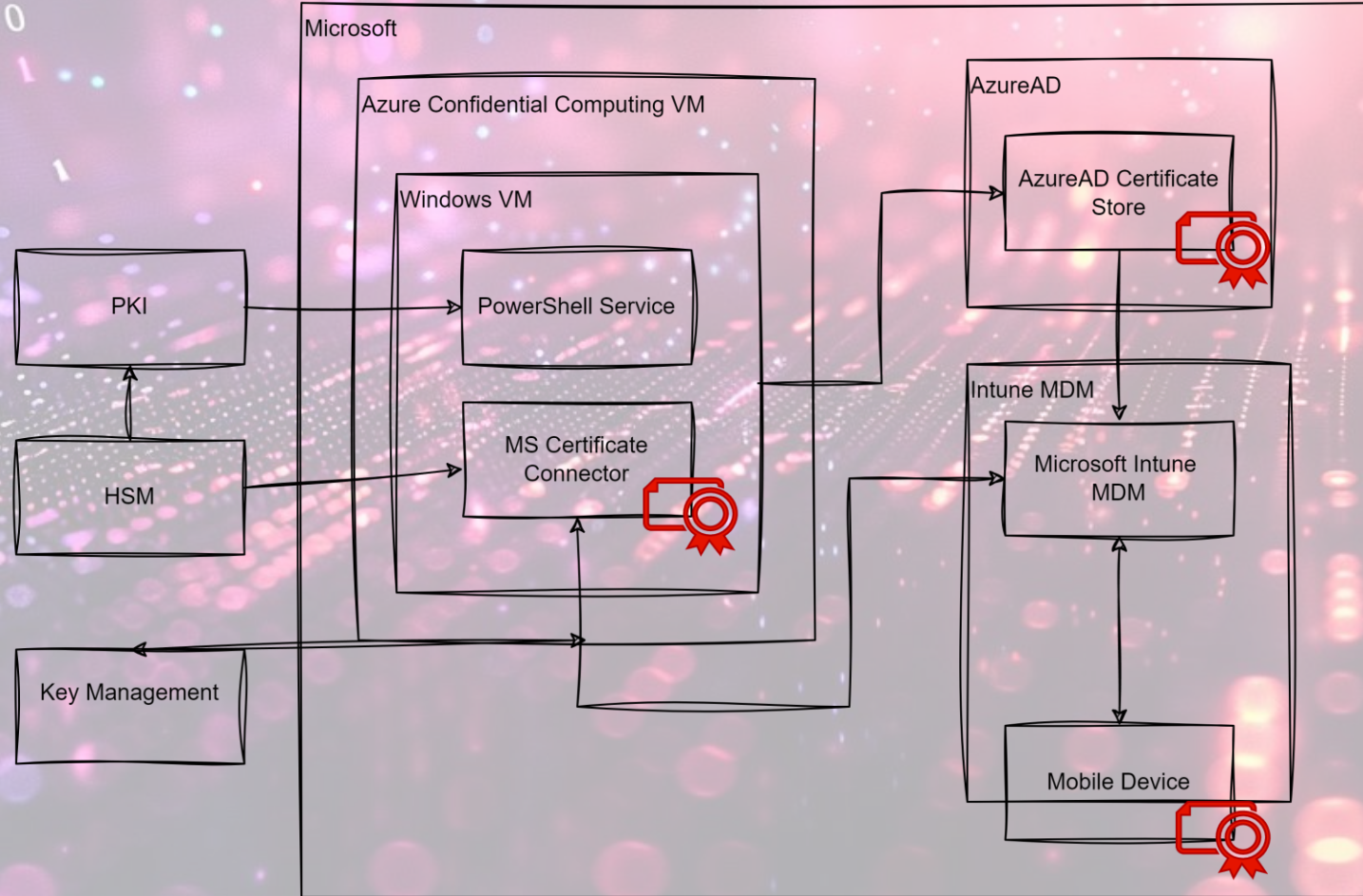


Pain points

- User certificates incl. private key are stored in AzureAD
- Outlook mobile
 - Only way to provision certificates to this app is via Intune
- MS Certificate Connector acts as kind of black box for Intune to re-encrypt all user certificates
- iOS only supported *TripleDES-SHA1* for pkcs#12 encryption only

No way to provision certificates without key priv. exposure

Architecture



Expirence in a nutshell

- Golive
 - Only small number of users recieved certificates on devices
 - 2nd import of the same certificates to EntraID -> fixed issue
 - Ticket ping-pong between vendors:
 - Apple <-> Microsoft
 - since 07/2024 it's working by magic, root cause never identified
- iOS only supports *TripleDES-SHA1* for pkcs#12 encryption
 - Deprecated by NIST in 2019
 - Fixed by Apple with iOS 18 beta2 ...

Expirence in a nutshell

- MIP vs S/MIME
 - Global configuration no device type specific configuration possible
 - Mobile: enc. Certificate
 - Non-Mobile: enc. + sig
- MS Certificate Connector process crashes min. once a week
 - Workarround, scheduled task to restart service.

A woman with long dark hair and glasses is shown from the chest up. She is holding a white mug. Her face is partially obscured by a digital overlay of binary code (0s and 1s) and other data-like patterns. The background is dark with some blurred lights. The text is overlaid on the center of the image.

***S/MIME the worst thing in the
universe?!?***

A woman with long dark hair and glasses is the central figure. Her face is partially obscured by a digital overlay of binary code and data streams, particularly around her eyes and the reflection in her glasses. She is holding a dark-colored mug in front of her. The background is a mix of dark and light blue tones with a bokeh effect. On the far left, there is a vertical film strip graphic with red and white frames.

Reality check.
Are our requirements wrong?!?

A woman with long dark hair and glasses is the central figure. Her face is partially obscured by a digital overlay of binary code (0s and 1s) and other data-like patterns. She is holding a dark-colored mug in front of her. The background is a mix of dark and light blue tones with a bokeh effect of out-of-focus lights. The overall aesthetic is high-tech and digital.

***Adding more complexity =
adding more security?***

A woman's face is the central focus, wearing dark-rimmed glasses. The lenses reflect a digital, binary-like pattern of glowing blue and white characters. She has long, dark hair. In the foreground, the top of a blue ceramic mug is visible. The background is a soft-focus mix of warm orange and yellow bokeh lights. The overall mood is technological and contemplative.

***Are we losing control of E2E
encryption?***

A woman with long dark hair is shown from the chest up, wearing black-rimmed glasses. The lenses of the glasses are filled with a complex, glowing digital data overlay consisting of various numbers, symbols, and lines of code. She is holding a white ceramic mug with a handle on the right side. The background is a soft-focus bokeh of red and blue lights, with a vertical strip of red light on the left side. The overall mood is technological and futuristic.

Only used by germans?

A woman with long dark hair is shown from the chest up, wearing dark-rimmed glasses. The lenses of the glasses reflect a complex digital code or data stream in shades of blue and white. She is holding a white ceramic mug with a handle on the right side. The background is a blurred mix of warm orange and yellow lights, suggesting an indoor setting with ambient lighting. The overall mood is futuristic and tech-oriented.

Future of S/MIME?

An aerial photograph of a dense forest of evergreen trees, likely spruce or fir, with varying shades of green and some yellowing foliage. The text 'Thank you' is overlaid in a large, white, italicized sans-serif font.

Thank you

e-on