# TeleTrusT-EBCA "PKI-Workshop" 2021

**Berlin, 30.09.2021**

# Uniper Use Case: Microsoft Information Protection vs. S/MIME

**Heino Rätscher, Uniper**

# Wichtige Daten

- Energieerzeuger (KRITIS Anforderungen)
- ca. 11.000 Mitarbeiter
- Windows 10 Clients
- ca. 5.000 Mobile Clients (Apple)
- Infrastruktur ca. 80% Cloud
- „Any Device – Any Network – Any Application“

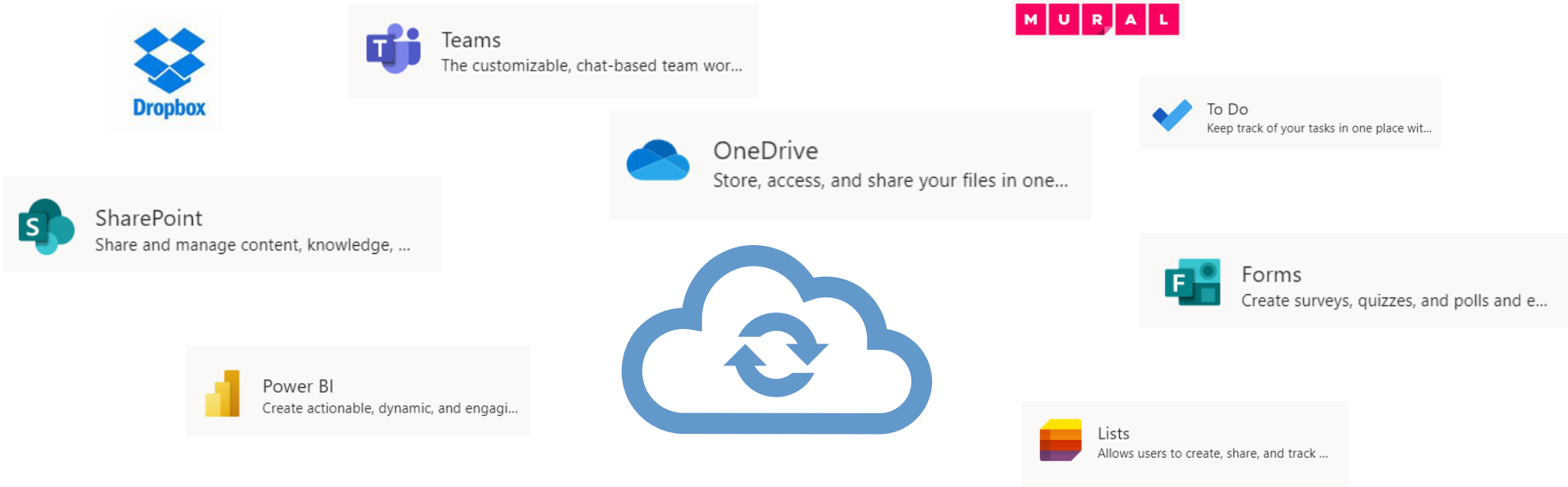
# Wie sah die „alte“ PKI Welt aus (ca. 2017)?

Streng vertrauliche Email


Sicherer Speicher (z. B. mit PKI Software verschlüsseltes Abteilungslaufwerk)

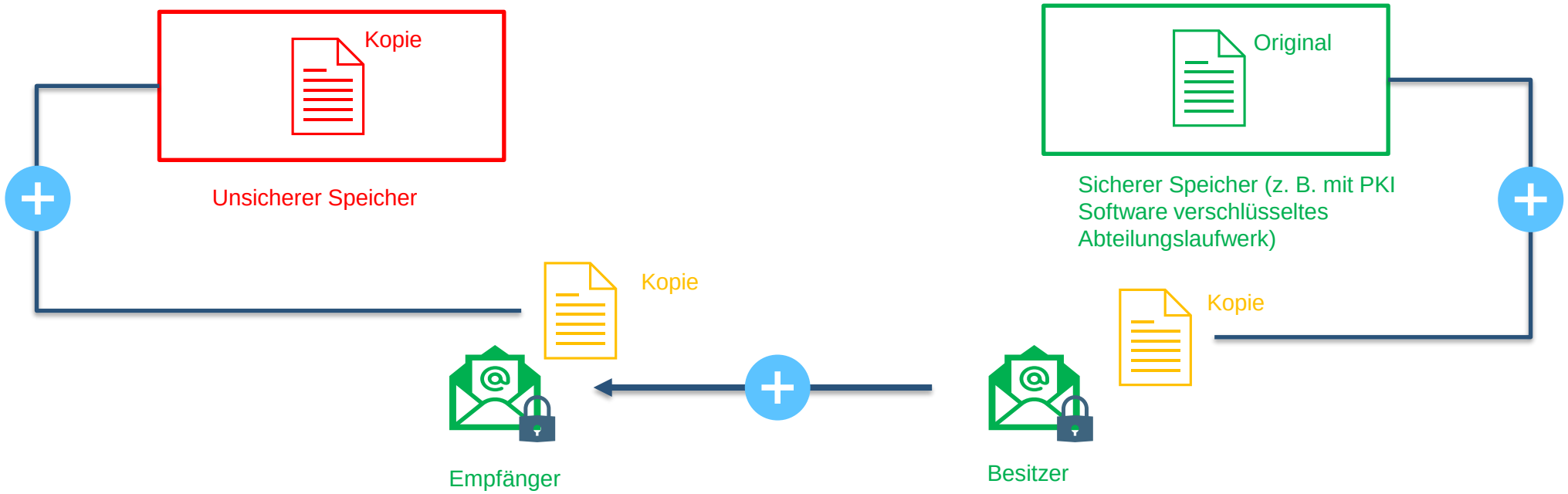
- PKI der Standard für Dokumente / Informationen mit erhöhtem Schutzbedarf
- PKI full-rollout (Enc / Sig / Auth)
- Größtenteils eigene Rechenzentren

# Was hat sich geändert dass PKI nicht mehr ausreichend war?



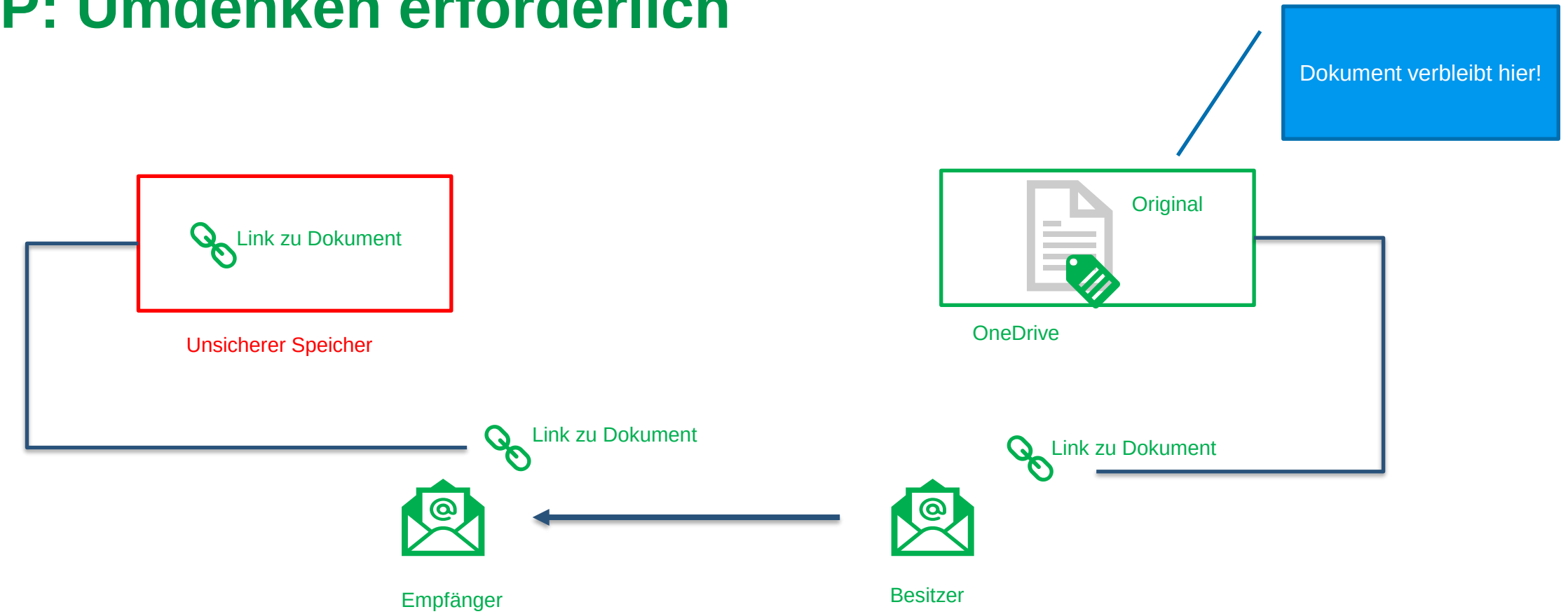

- Wie in vielen Fällen: es kam die Cloud..
  - Microsoft Office bestand nicht mehr nur aus Excel, Word und Co.
- Datenspeicher- und Austauschorte haben massiv zugenommen (Dropbox, usw..)
- Höhere Flexibilität gefordert (any Device)

# War PKI überhaupt die richtige Lösung zum Schutz von Dokumenten / Informationen?




- In den allermeisten Fällen wird ein Dokument dazu erstellt, um mit anderen geteilt zu werden
- Daten wurden vervielfältigt und waren selbst nicht geschützt
- Vertrauliche Informationen nicht mehr nur in Dateien (z.b. Chats, online Whiteboards,..)

# MIP: Umdenken erforderlich




- Keine mehrfachen Kopien eines Dokumentes, Platzersparnis
- Zentrale Berechtigungsverwaltung
- Gemeinsames Bearbeiten desselben Dokumentes, Zeitersparnis
- Speicherort selbst ist nicht mehr ganz so wichtig, da Schutz auf dem Dokument liegt (falls dies doch mal multipliziert wird)

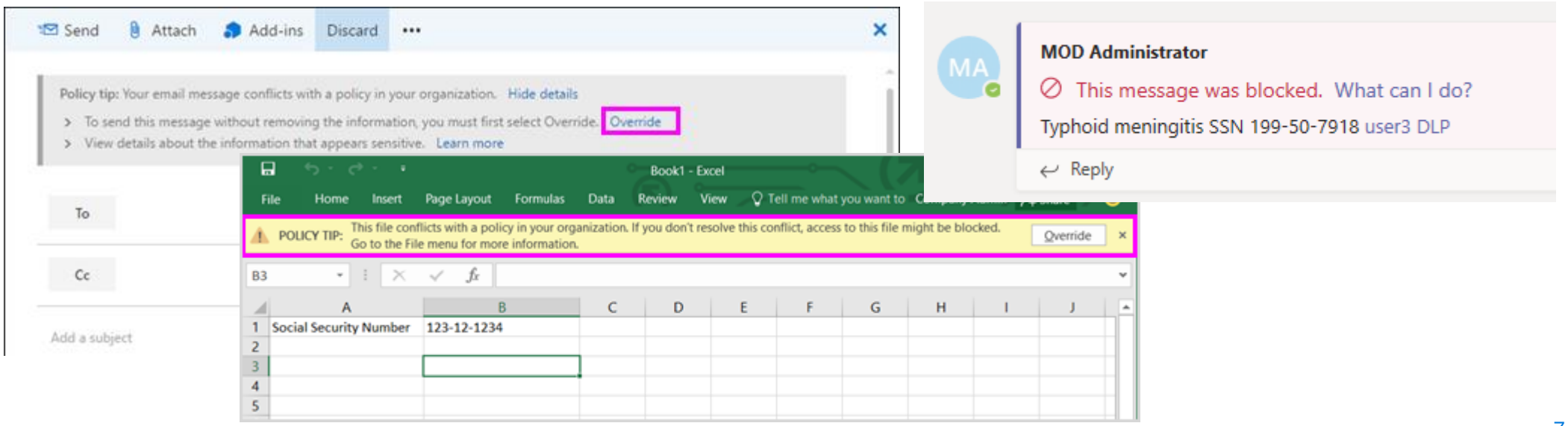
# Wesentliche Unterschiede MIP vs. S/MIME

- MIP – Ein Ersatz zum Dokumenten- und Informationsschutz, nicht für Authentifizierung oder digitale Signatur (daher auch der Name „Information Protection“)
- Schutz von Informationen auch außerhalb Word, Excel und Co. (Sharepoint, Teams chats)
- Wachsende Unterstützung der MIP Labels durch andere Hersteller (z.B. Adobe)
- Mehr als nur Transport und Ablageschutz. Verhindern das eine Information weitergeleitet wird, ausgedruckt oder über Teams in einer Session geteilt wird.
- Mehr Flexibilität – Dokumente können weiterhin gesucht werden in OneDrive und Co.
- Funktion „out-of-the-box“ verfügbar von Microsoft, keine zusätzlichen Add-ins erforderlich zur Unterstützung.
- Keine 1:1 Verschlüsselung mehr per default
- (Noch) nicht vollständig kompatibel mit Gruppenpostfächern
- Automatisierung schwierig

# MIP Labels ist nur ein kleiner Teil der Gesamtlösung

Weitergehender Schutz mit MCAS (Microsoft Cloud App Security) und DLP (Data Loss Prevention)

- Bestimmen welches Dokument über welche Plattform geteilt werden darf
- Verhindern das als „intern“ gekennzeichnete Dokumente extern geteilt und versendet werden
- (Automatisierte) Suche, Überwachung und Klassifizierung von Dokumenten mit kritischen Informationen (z.B. Personalausweis Nummer, Gesundheitsdaten)
- Verhinderung von Datenverlust durch automatisierte Information des Anwenders wenn in einem Dokument / Email z.B. eine Personalausweis Nummer erkannt wird.
  - Kann auch vorgegeben werden und Dokument automatisch geschützt / geblockt werden
- Retention: Daten automatisch löschen nach bestimmter Zeit



# Erfahrungen und Lessons learned

- Gründliche Information bevor man anfängt
  - Konzept erstellen
  - Wer verwaltet wie den MIP Schlüssel? (BYOK,…)
  - Klare Prozesse und Organisation (Wer ist für was verantwortlich)
- Früher an später denken,
  - Was, wenn ein Mitarbeiter ausscheidet?
  - Migration von Daten von einem Unternehmen zum anderen (z.B. beim Verkauf)?
- Gründlich Gedanken machen bezüglich Labels
  - Eine spätere Änderung ist sehr schwer umzusetzen. Nicht nur technisch sondern auch zwecks Aufwand Kommunikation usw.
  - Labels so gering wie möglich halten (Empfehlung auch von MS)
  - So gut wie möglich custom permissions vermeiden
  - Kein Strictly Confidential Domain label
- Schulung und Kommunikation sehr wichtig
  - Wie kann ich ein Dokument teilen und nicht per Mail versenden
  - Wie und wo vergebe ich die Berechtigungen

Author: Heino Rätscher, Digital Workplace Security Architect, Uniper