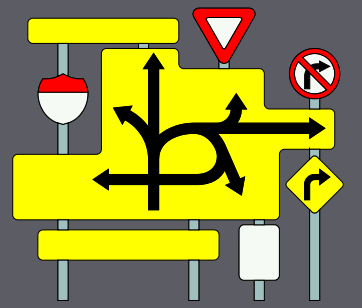
LAYER SECURITY

# E2EE – End to End Encryption

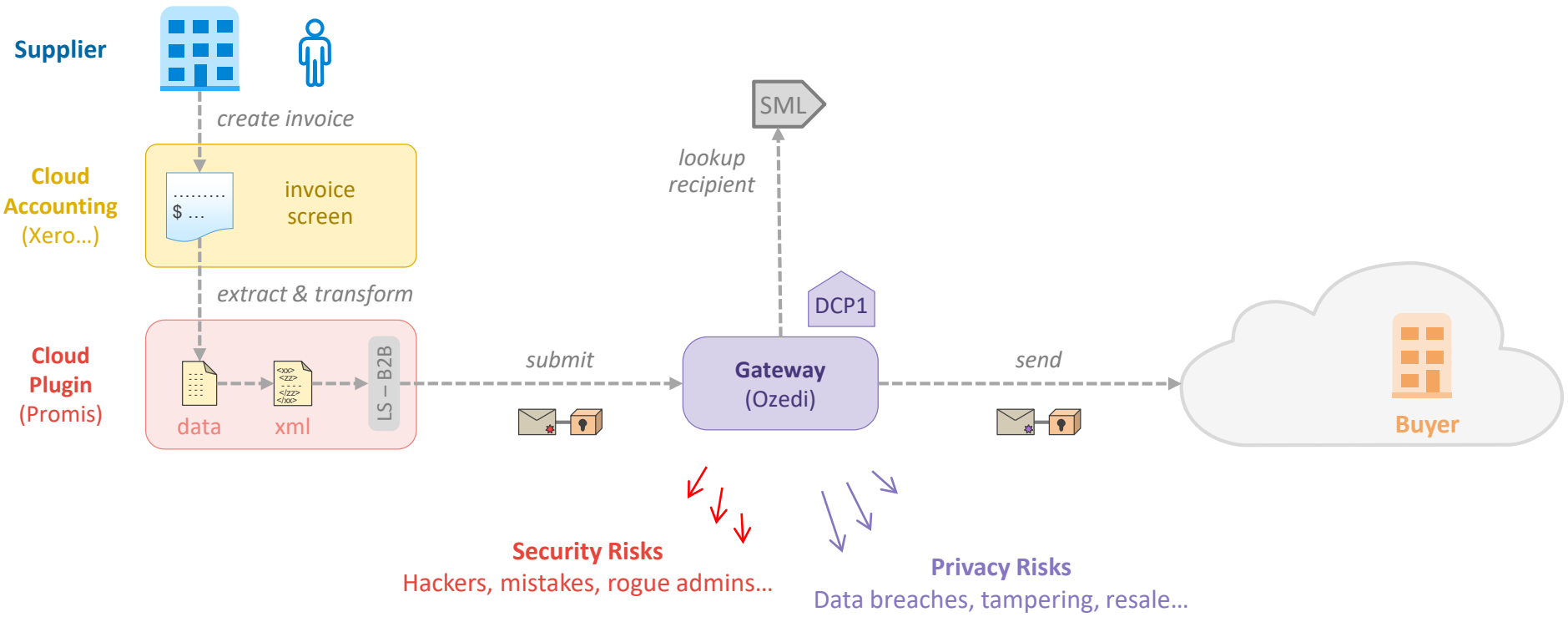
PEPPOL, Brussels, October 2019



**Rick Harvey** FIEAust FACS

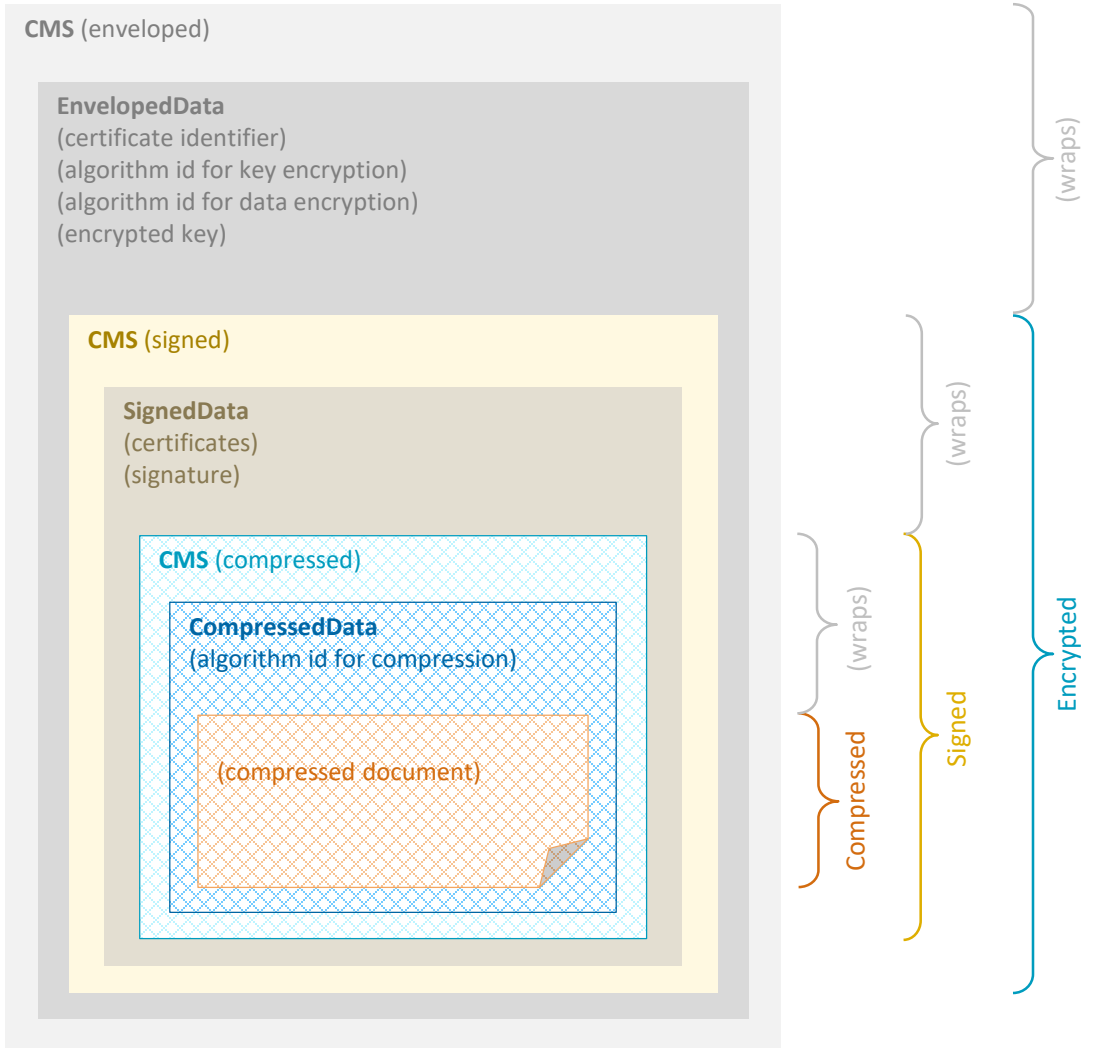
CEO & Founder, Layer Security

# Corner 1.5



# CMS

- **CMS – Cryptographic Message Syntax**
  - International standard
    - CMS, PKCS#7, RFC5652
  - Widely used
    - e.g. S/MIME (superset), P7B Cert Chain (subset)



# CMS – Easy

- **Package**
  - Layered wrapping
    - Compress, sign, encrypt
    - 3 OpenSSL commands!

```
# Create CMS (compress, sign, encrypt)
openssl cms -compress -binary -in doc1.txt -outform der -out doc1-c.cms
openssl cms -sign -binary -nodetach -noattr -md sha256 -in doc1-c.cms -signer user1.crt -inkey user1.key -passin pass:Password1! -outform der -out doc1-cs.cms
openssl cms -encrypt -binary -aes128 -in doc1-cs.cms -outform der -out doc1-cse.cms user2.crt

# Extract CMS (decrypt, verify, uncompress)
openssl cms -decrypt -inform der -in doc2-cse.cms -keyform pem -inkey user2.key -passin pass:Password1! -outform der -out doc2-cs.cms
openssl cms -verify -inform der -in doc2-cs.cms -outform der -CAfile root.crt -out doc2-c.cms
openssl cms -uncompress -inform der -in doc2-c.cms -outform der -out doc2.txt
```

LAYER SECURITY

# Questions?