IBE and S/MIME

Russ Housley
Founder of Vigil Security, LLC
Chair of IETF

Vigil Security LLC

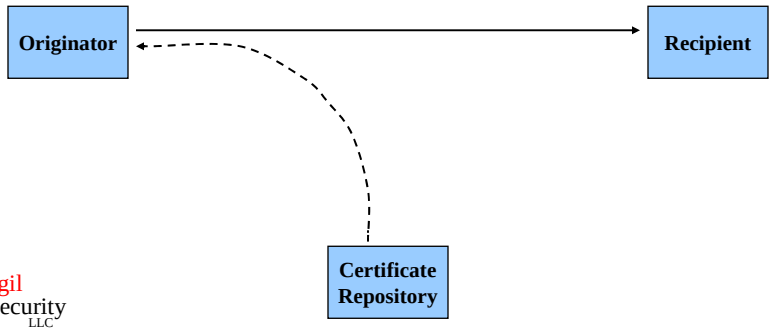
Adding New Algorithms

- Algorithm standards are just the beginning
- Modern security protocols are algorithm agile, but each protocol needs to be profiled to use each algorithm
- Innovative new algorithms may require the use of protocol extensions or support infrastructure to take advantage of unforeseen capabilities

Vigil Security LLC

Traditional S/MIME Encryption

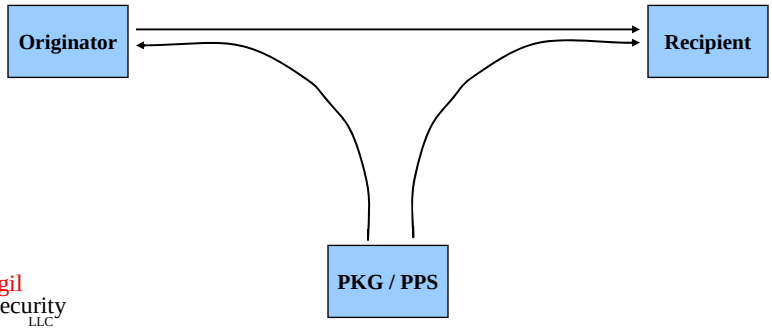
1. Originator fetches the certificate
   (or saves it from an earlier message)
2. Originator sends the encrypted message



Vigil Security LLC

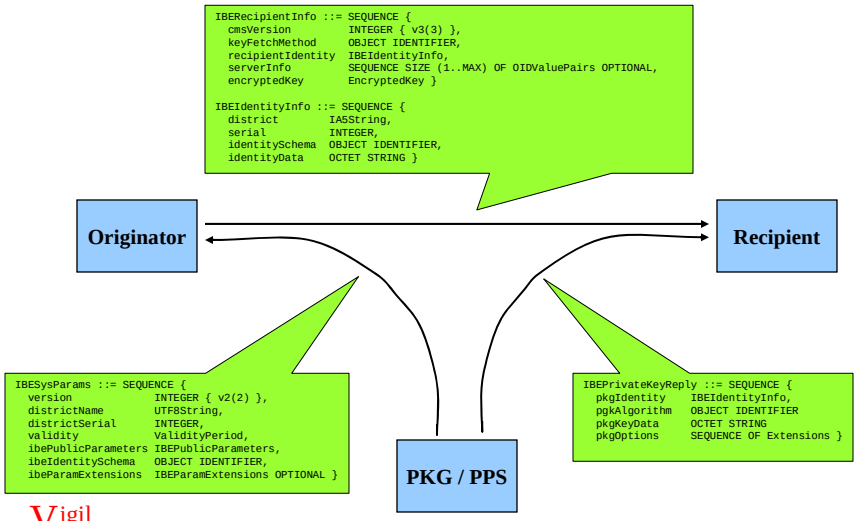
IBE S/MIME Encryption

1. Originator fetches the IBE Public Parameters
2. Originator sends the encrypted message
3. Recipient fetches their IBE private key



Vigil Security LLC

IBE S/MIME Encryption



Vigil Security LLC

Interoperability is the Goal

- Interoperable use of new algorithms means:
  - Algorithm standards
  - Specification of syntax and elements of procedure to use the new algorithm in existing security protocols

Vigil Security LLC

Questions?

Russ Housley
housley@vigilsec.com

Vigil Security LLC