

Extending Derived Credential with S/MIME Support



Encryption & Mobility Challenges

- E-mail encryption with Smart Card poses significant challenges for mobility
 - While desktop and laptop computing devices can easily be equipped with smart card readers, the same option is not practical for mobile devices
- Currently, many companies and agencies encrypt e-mail using soft keys that can reside on any computing platform, including mobile
- In the government, PIV encryption keys is typically protected by Medium-Hardware policy, which complicates key delivery to mobile devices
- Lack of practical solutions to address encryption and mobility may prevent companies and agencies from adopting encryption with Smart Card keys

NIST SP 800-157 (Derived Credential)

- NIST SP 800-157 defines technical specifications for implementing and deploying derived credentials to mobile devices
- While derived credentials are suitable for authentication, currently the actual keys are required to read encrypted email on mobile devices
- Many vendors developed solutions based on SP 800-157 specifications, but no solution addresses encryption/decryption with Medium-Hardware protection policy (Level 4)
- Two kinds of solutions are available for mobility and encryption:
 - Allow keys to be recovered, which is not suitable for Level 4 protected keys
 - Generate an encryption derived key pairs, which doesn't allow for decryption

Ahead of The Curve Solution

- Extends derived credentials to enable sending and receiving encrypted mail on mobile devices without an attached Smart Card reader
- Can be integrated with any mobile device management (MDM) solution
- Works for any mobile device supported by the MDM solution
 - Android, iOS, BlackBerry, & Windows
- A server solution with nothing to install or configure on mobile devices
- Based on MobileDecrypt header modification technology
 - Insert user's encrypted derived certificate into the encrypted message header

PKI Encryption Overview (RFC 2315)

Legend


c: Client (aka user)

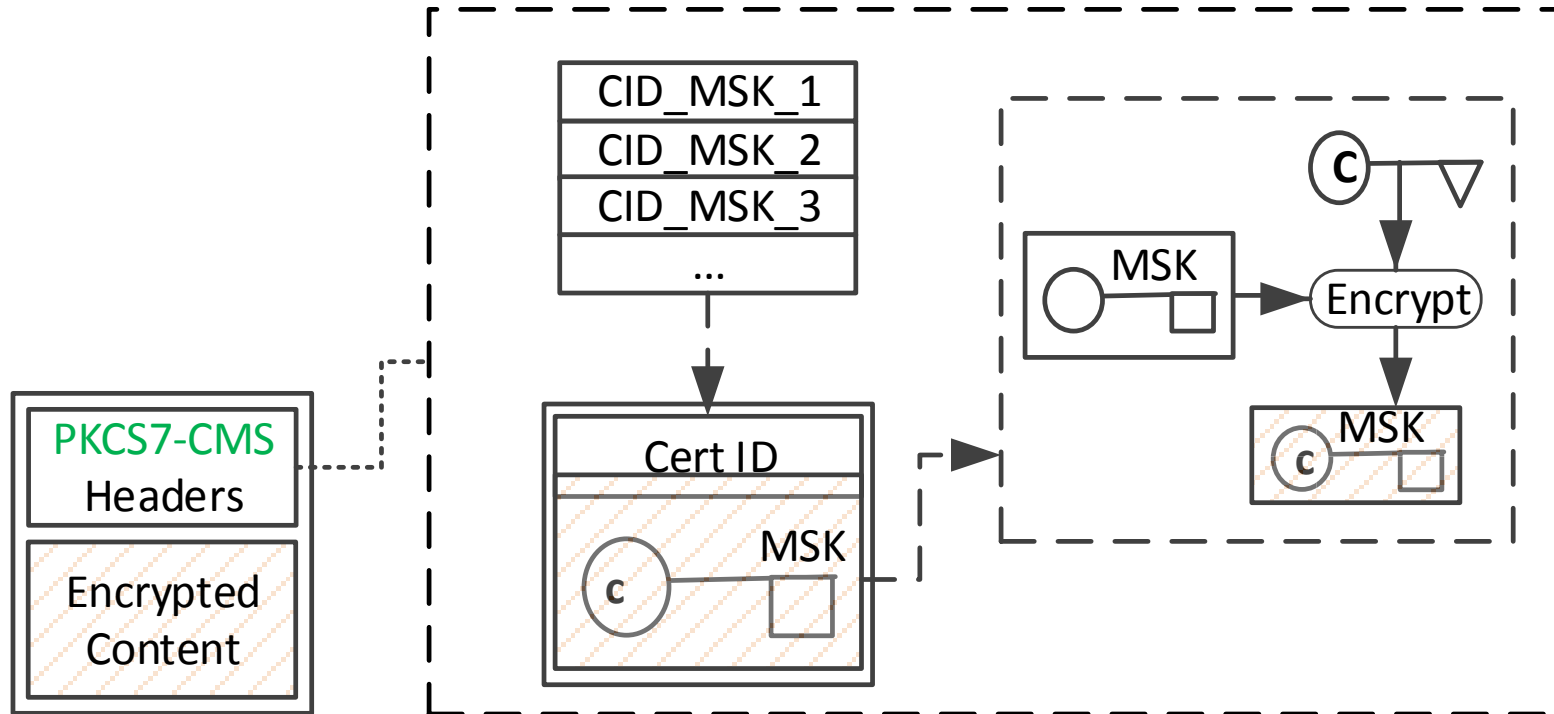
MSK: Message Session Key

CID_MSK_#: Cert ID and Message Session Key

Public Key: 

Symmetric Key: 

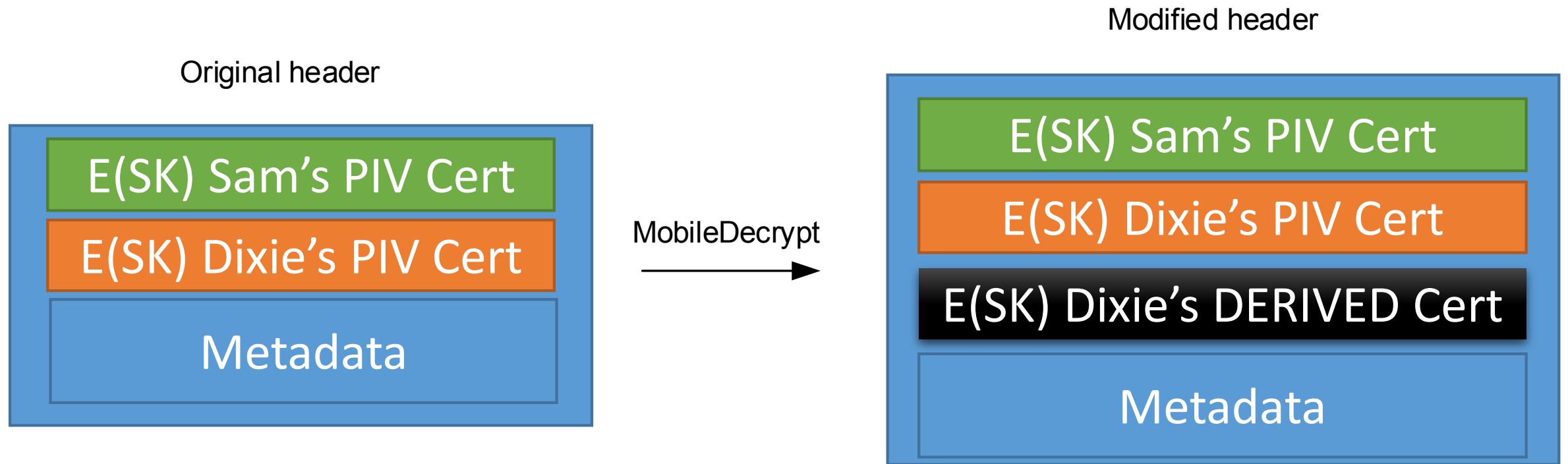
Encrypted: 



Steps required for encryption

- Generate Message Session Keys (MSK) and use it to encrypt content
- Encrypt the MSK with recipients Public Keys as part of the message header

MobileDecrypt Header Modification

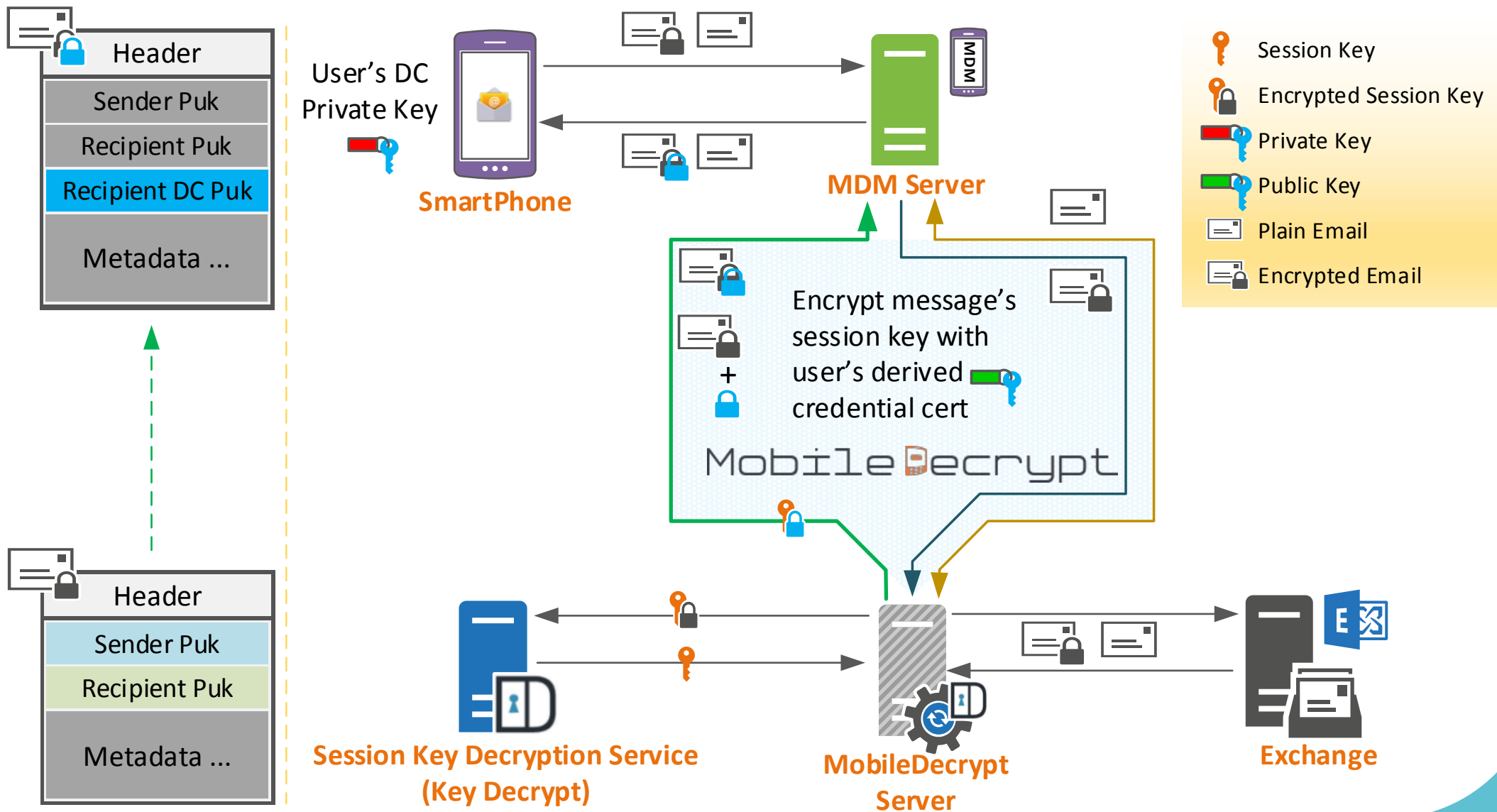


■ Header Modification steps

- Use a Session Key Decryption service to retrieve message Session Key (SK)
- Encrypt message (SK) using user's configured encryption derived certificate
- Re-assemble encrypted message header

MobileDecrypt High-level Architecture

MobileDecrypt High-level Architecture



DecryptNaBox Technology

DecryptNaBox delivers access to encrypted email without compromising security

Data encryption usage is increasing to meet regulatory and security concerns. DecryptNaBox enables organizations to maintain the security of the certificate authority while providing access for eDiscovery and security processes.



SUPPORTS GOVERNMENT AND INDUSTRY REQUIREMENTS

- eDiscovery
- Data leakage protection
- 01011
- MobileDecrypt
- Virus scanning at the edge

- Separation of data decryption from keys
- Integrated Hardware Security Module (HSM) for key protection and FIPS140-2 compliance
- Support for multiple Certificate Authorities
- High volume data decryption service that operates without access to Private Keys

Microsoft Case study: <https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=21292>

Demo

