Apps: *Architecture*
SAAG: *Security*
Considerations

Trust & Security Considerations

L. Levison
D. Crocker

PRIME: Privacy Respecting Internet Mail Environment

Internet Engineering Task Force Ninety-Two

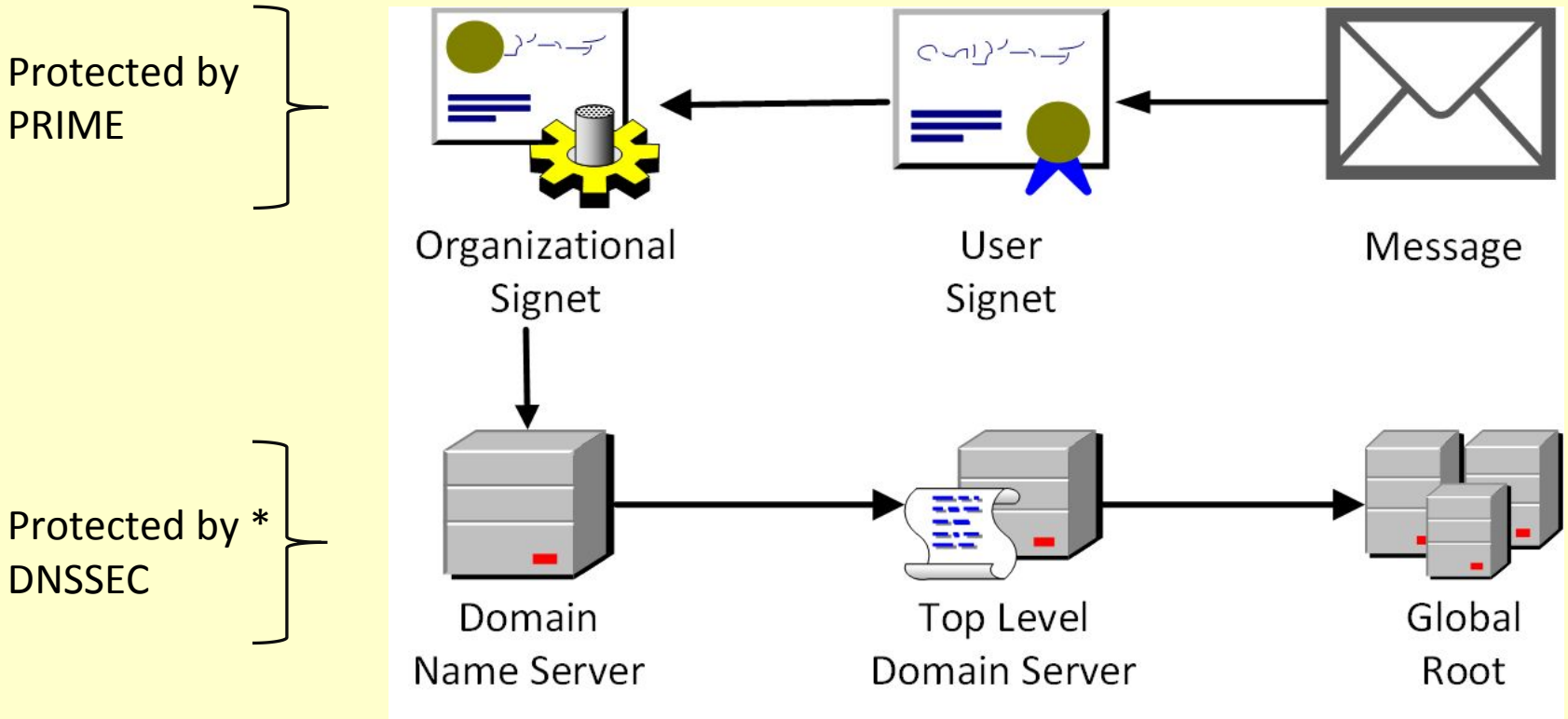
Design Goals

- Secure communications platform for asynchronous messaging
- Distinguished by automated key management
- Uses layers of message-based end-to-end* encryption
- Provides message confidentiality, tamper protection and reduces the leakage of metadata along the handling path
- Strives to make security dependent on the complexity of a user's password and strength of their endpoint's defenses

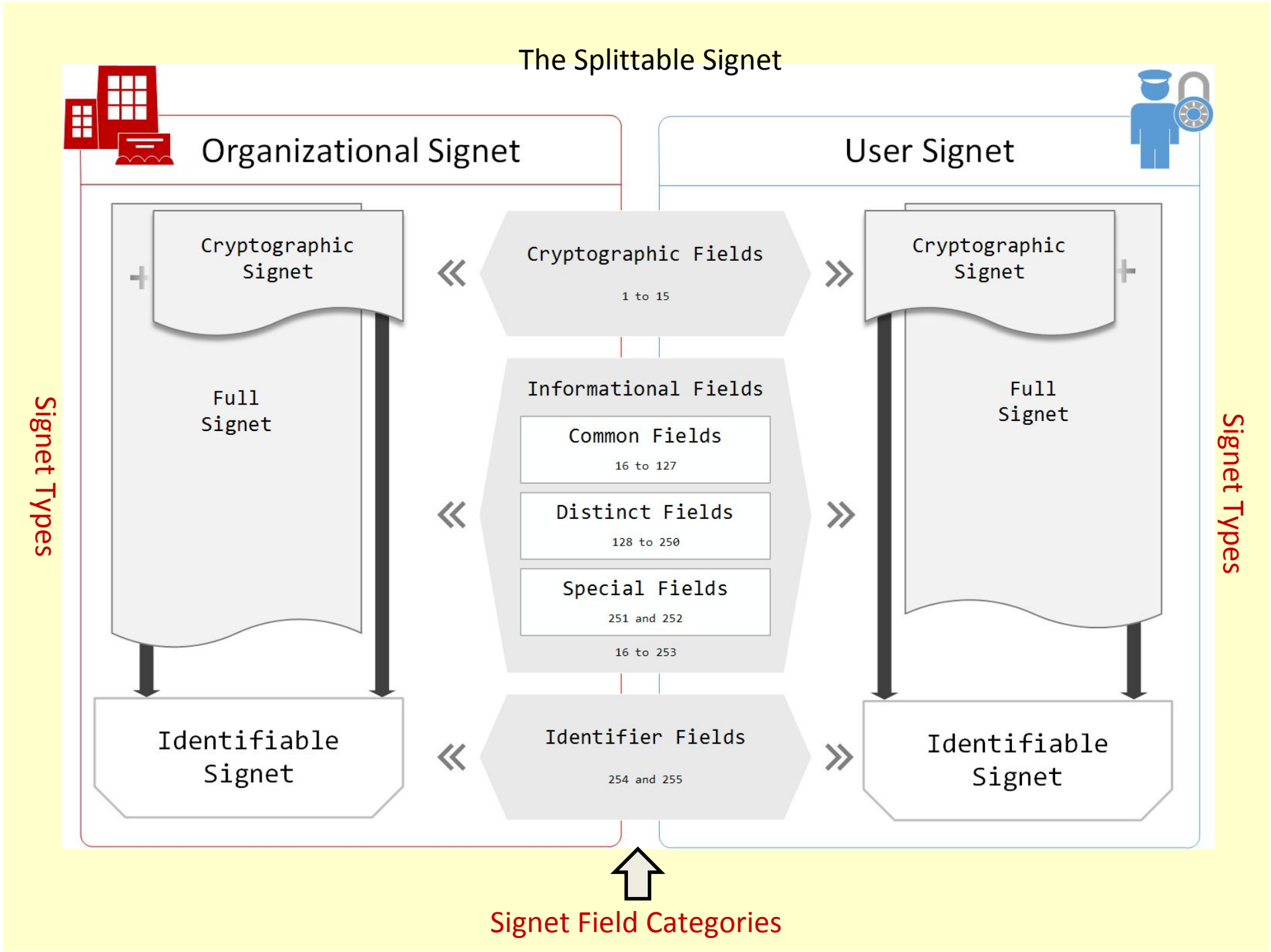
* Automation allows the "end" to be a user's device, or server

Trust Model

Signet resolver obtains a signet from an authoritative primary source and then validates it using a pre-authenticated secondary source.



* DNSSEC does not protect the confidentiality of queries, and is dependent upon the austerity of the controlling authorities.

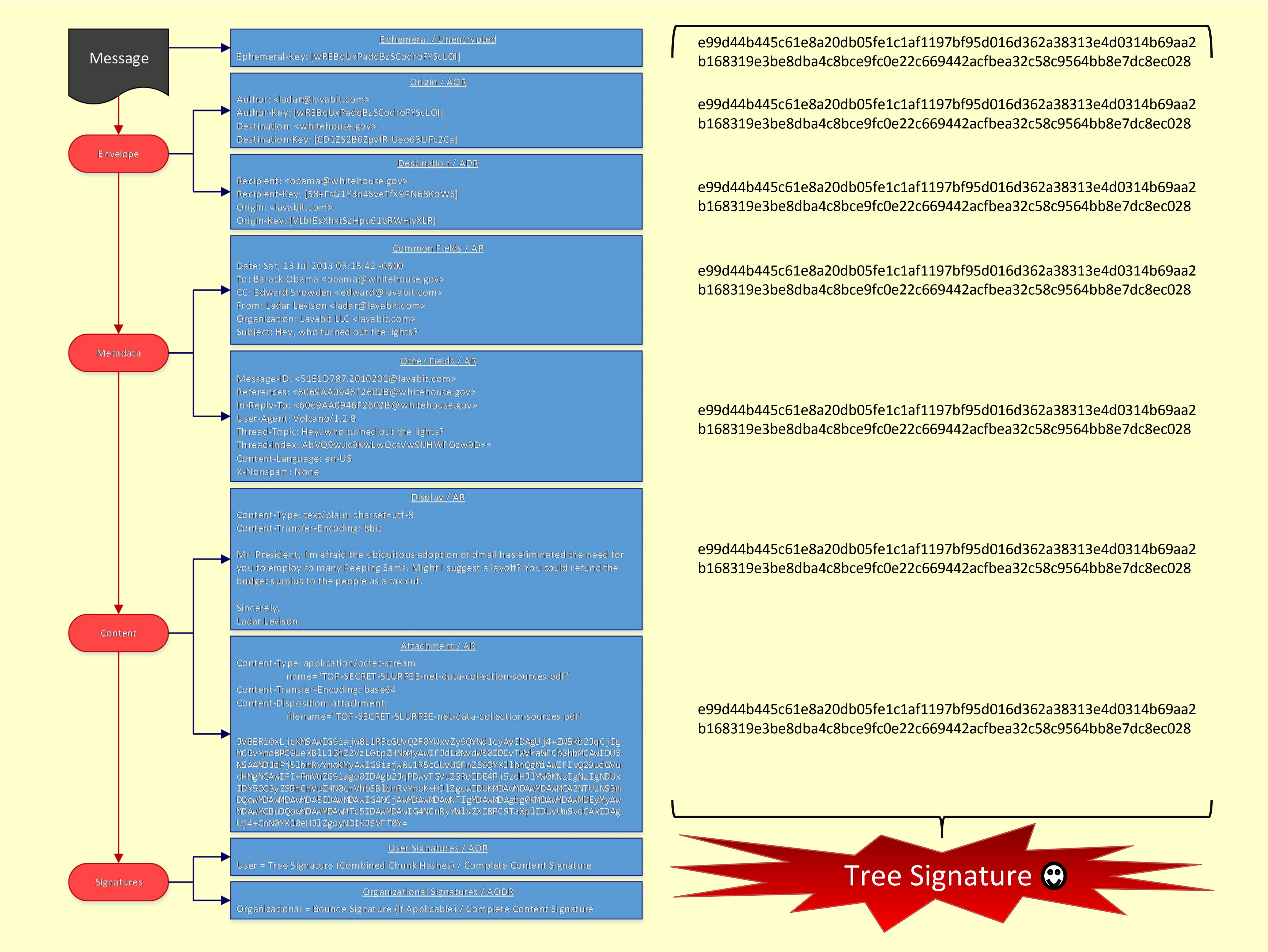

The Splittable Signet
Organizational Signet
User Signet
Signet Types
Signet Types
Cryptographic Signet
Full Signet
Cryptographic Fields
1 to 15
Informational Fields
Common Fields
16 to 127
Distinct Fields
128 to 250
Special Fields
251 and 252
16 to 253
Identifier Fields
254 and 255
Cryptographic Signet
Full Signet
Identifiable Signet
Identifiable Signet
Signet Field Categories

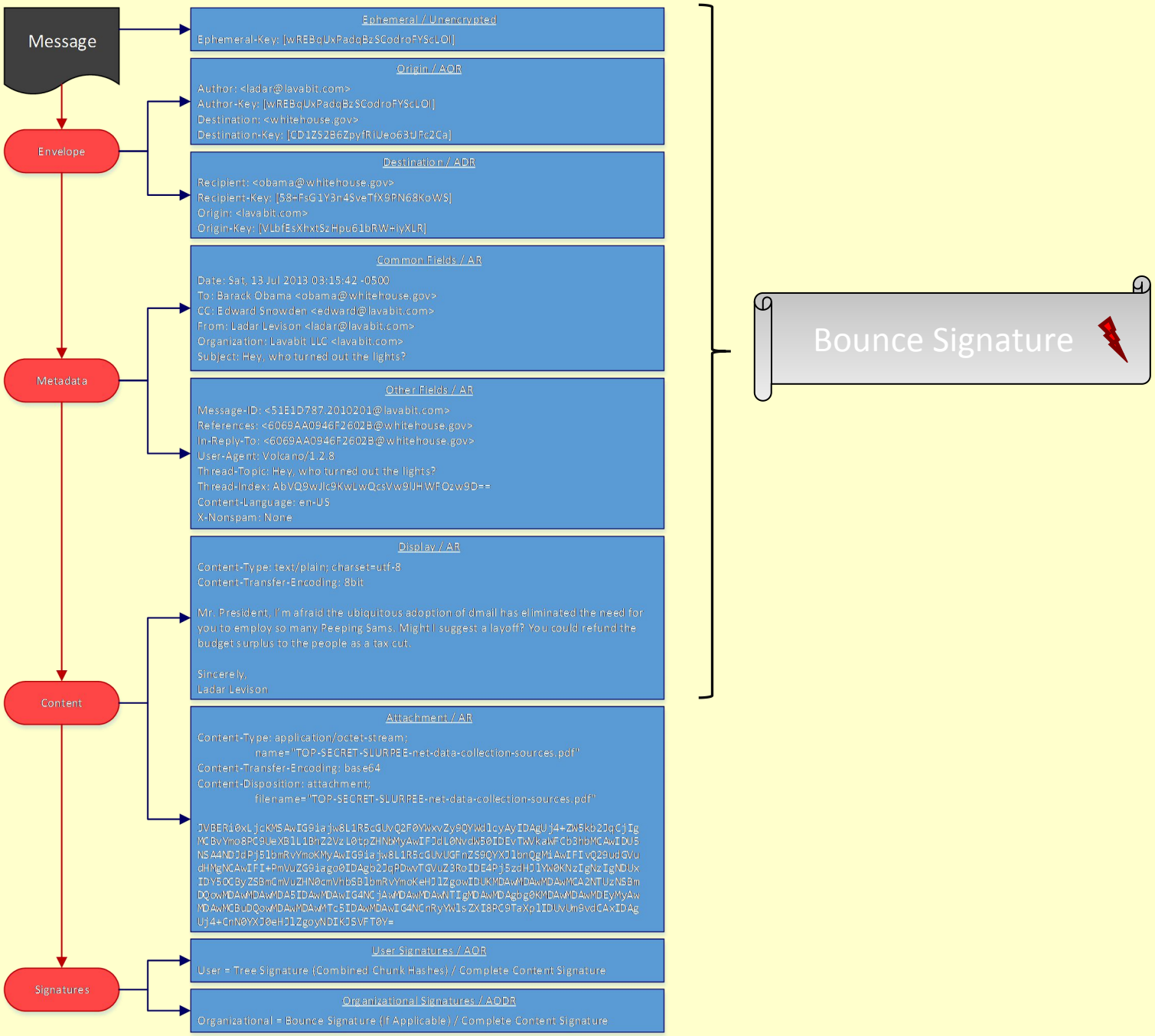
Algorithms

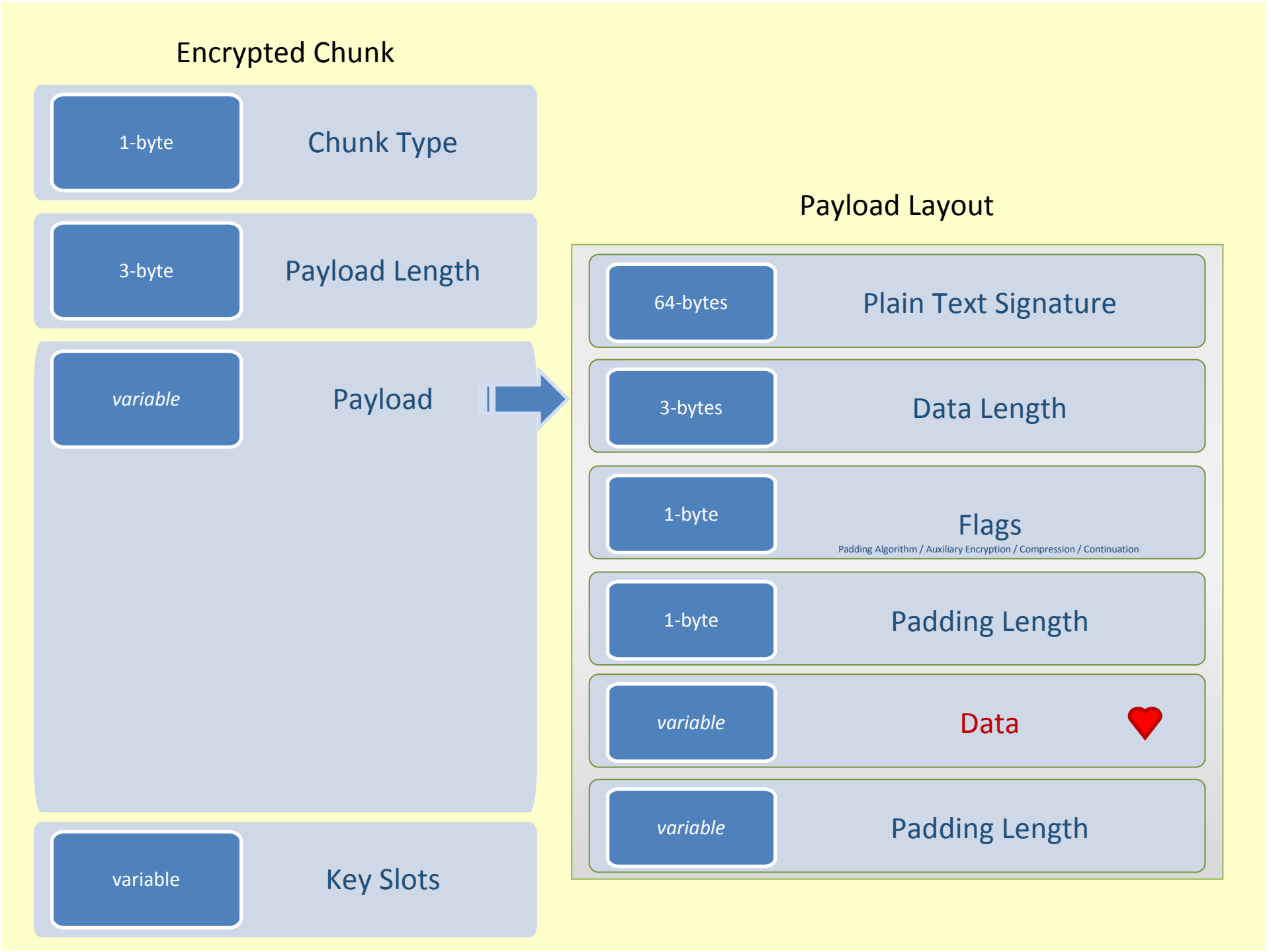
Transport Layer	
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Certificate Strength	2048+
Curve	*unspecified*

Signets		
Signing	EdDSA	Ed25519

Messages		
ASYMMETRIC	ECDHE	SECP256K1
KDF	SHA-2	SHA-512
SYMMETRIC	AES	CBC-256
SIGN/MAC	EdDSA	Ed25519


Message
Envelope
Metadata
Content
Signatures
Ephemeral / Unencrypted
Ephemeral-Key: [wREBqUxPadqBzSCodroFYScLOI]
Origin / AOR
Author: <ladar@lavabit.com>
Author-Key: [wREBqUxPadqBzSCodroFYScLOI]
Destination: <whitehouse.gov>
Destination-Key: [CD1ZS2B6ZpyfRiUeo63tJFc2Ca]
Destination / ADR
Recipient: <obama@whitehouse.gov>
Recipient-Key: [58+FsG1Y3n4SveTfX9PN68KoWS]
Origin: <lavabit.com>
Origin-Key: [VLbfEsXhxtSzHpu61bRW+iyXLR]
Common Fields / AR
Date: Sat, 13 Jul 2013 03:15:42 -0500
To: Barack Obama <obama@whitehouse.gov>
CC: Edward Snowden <edward@lavabit.com>
From: Ladar Levison <ladar@lavabit.com>
Organization: Lavabit LLC <lavabit.com>
Subject: Hey, who turned out the lights?
Other Fields / AR
Message-ID: <51E1D787.2010201@lavabit.com>
References: <6069AA0946F2602B@whitehouse.gov>
In-Reply-To: <6069AA0946F2602B@whitehouse.gov>
User-Agent: Volcano/1.2.8
Thread-Topic: Hey, who turned out the lights?
Thread-Index: AbVQ9wJlc9KwLwQcsVw9lJHWFOzw9D==
Content-Language: en-US
X-Nonspam: None
Display / AR
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit
Mr. President, I'm afraid the ubiquitous adoption of dmail has eliminated the need for you to employ so many Peeping Sams. Might I suggest a layoff? You could refund the budget surplus to the people as a tax cut.
Sincerely,
Ladar Levison
Attachment / AR
Content-Type: application/octet-stream;
name="TOP-SECRET-SLURPEE-net-data-collection-sources.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="TOP-SECRET-SLURPEE-net-data-collection-sources.pdf"
JVBERi0xLjcKMSAwIG9iajw8L1R5cGUvQ2F0YWxvZy9QYWdlcyAyIDAgUj4+ZW5kb2JqCjIg
MCBvYmo8PC9UeXBlL1BhZ2VzL0tpZHNbMyAwIFJdL0NvdW50IDEvTWVkaWFCb3hbMCAwIDU5
NSA4NDJdPj5lbmRvYmoKMyAwIG9iajw8L1R5cGUvUGFnZS9QYXJlbnQgMiAwIFIvQ29udGVu
dHMgNCAwIFI+PmVuZG9iago0IDAgb2JqPDwvTGVuZ3RoIDE4Pj5zdHJlYW0KNzIgNzIgNDUx
IDY5OCByZSBmCmVuZHN0cmVhbSBlbmRvYmoKeHJlZgowIDUKMDAwMDAwMDAwMCA2NTUzNSBm
DQowMDAwMDAwMDA5IDAwMDAwIG4NCjAwMDAwMDAwNTIgMDAwMDAgbg0KMDAwMDAwMDEyMyAw
MDAwMCBuDQowMDAwMDAwMTc5IDAwMDAwIG4NCnRyYWlsZXI8PC9TaXplIDUvUm9vdCAxIDAg
Uj4+CnN0YXJ0eHJlZgoyNDIKJSVFT0Y=
User Signatures / AOR
User = Tree Signature (Combined Chunk Hashes) / Complete Content Signature
Organizational Signatures / AODR
Organizational = Bounce Signature (If Applicable) / Complete Content Signature
e99d44b445c61e8a20db05fe1c1af1197bf95d016d362a38313e4d0314b69aa2
b168319e3be8dba4c8bce9fc0e22c669442acfbea32c58c9564bb8e7dc8ec028
e99d44b445c61e8a20db05fe1c1af1197bf95d016d362a38313e4d0314b69aa2
b168319e3be8dba4c8bce9fc0e22c669442acfbea32c58c9564bb8e7dc8ec028
e99d44b445c61e8a20db05fe1c1af1197bf95d016d362a38313e4d0314b69aa2
b168319e3be8dba4c8bce9fc0e22c669442acfbea32c58c9564bb8e7dc8ec028
e99d44b445c61e8a20db05fe1c1af1197bf95d016d362a38313e4d0314b69aa2
b168319e3be8dba4c8bce9fc0e22c669442acfbea32c58c9564bb8e7dc8ec028
e99d44b445c61e8a20db05fe1c1af1197bf95d016d362a38313e4d0314b69aa2
b168319e3be8dba4c8bce9fc0e22c669442acfbea32c58c9564bb8e7dc8ec028
e99d44b445c61e8a20db05fe1c1af1197bf95d016d362a38313e4d0314b69aa2
b168319e3be8dba4c8bce9fc0e22c669442acfbea32c58c9564bb8e7dc8ec028
e99d44b445c61e8a20db05fe1c1af1197bf95d016d362a38313e4d0314b69aa2
b168319e3be8dba4c8bce9fc0e22c669442acfbea32c58c9564bb8e7dc8ec028
Tree Signature


Message
Envelope
Metadata
Content
Signatures
Ephemeral / Unencrypted
Ephemeral-Key: [wREBqUxPadqBzSCodroFYScLOI]
Origin / AOR
Author: <ladar@lavabit.com>
Author-Key: [wREBqUxPadqBzSCodroFYScLOI]
Destination: <whitehouse.gov>
Destination-Key: [CD1ZS2B6ZpyfRiUeo63UFc2Ca]
Destination / ADR
Recipient: <obama@whitehouse.gov>
Recipient-Key: [58+FsG1Y3n4SveTfX9PN68KoWS]
Origin: <lavabit.com>
Origin-Key: [VLbfEsXhxtSzHpu61bRW+iyXLR]
Common Fields / AR
Date: Sat, 13 Jul 2013 03:15:42 -0500
To: Barack Obama <obama@whitehouse.gov>
CC: Edward Snowden <edward@lavabit.com>
From: Ladar Levison <ladar@lavabit.com>
Organization: Lavabit LLC <lavabit.com>
Subject: Hey, who turned out the lights?
Other Fields / AR
Message-ID: <51E1D787.2010201@lavabit.com>
References: <6069AA0946F2602B@whitehouse.gov>
In-Reply-To: <6069AA0946F2602B@whitehouse.gov>
User-Agent: Volcano/1.2.8
Thread-Topic: Hey, who turned out the lights?
Thread-Index: AbVQ9wJlc9KwLwQcsVw9IJHWFOzw9D==
Content-Language: en-US
X-Nonspam: None
Display / AR
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 8bit
Mr. President, I'm afraid the ubiquitous adoption of dmail has eliminated the need for you to employ so many Peeping Sams. Might I suggest a layoff? You could refund the budget surplus to the people as a tax cut.
Sincerely,
Ladar Levison
Attachment / AR
Content-Type: application/octet-stream;
name="TOP-SECRET-SLURPEE-net-data-collection-sources.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="TOP-SECRET-SLURPEE-net-data-collection-sources.pdf"
JVBERi0xLjcKMSAwIG9iajw8L1R5cGUvQ2F0YWxvZy9QYWdlcyAyIDAgUj4+ZW5kb2JqCjIg
MCBvYmo8PC9UeXBlL1BhZ2VzL0tpZHNbMyAwIFJdL0NvdW50IDEvTWVkaWFCb3hbMCAwIDU5
NS44NDJdPj5lbmRvYmoKMyAwIG9iajw8L1R5cGUvUGFnZS9QYXJlbnQgMiAwIFIvQ29udGVu
dHMgNCAwIFI+PmVuZG9iago0IDAgb2JqPDwvTGVuZ3RoIDE4Pj5zdHJlYW0KNzIgNzIgNDUx
IDY5OCByZSBmCmVuZHN0cmVhbGlbmRvYmoKeHJlZgowIDUKMDAwMDAwMDAwMCA2NTUzNSBm
DQowMDAwMDA5IDAwMDAwIG4gNCjAwMDAwMDAwNTIgMDAwMDAgbg0KMDAwMDAwMDEyMyAw
MDAwMCBuDQowMDAwMDAwMTc5IDAwMDAwIG4NCnRyYWlsZXI8PC9TaXplIDUvUm9vdCAxIDAg
Uj4+CnN0YXJ0eHJlZgoyNDIKJSVFT0Y=
User Signatures / AOR
User = Tree Signature (Combined Chunk Hashes) / Complete Content Signature
Organizational Signatures / AODR
Organizational = Bounce Signature (If Applicable) / Complete Content Signature
Bounce Signature


Encrypted Chunk
1-byte
Chunk Type
3-byte
Payload Length
variable
Payload
variable
Key Slots
Payload Layout
64-bytes
Plain Text Signature
3-bytes
Data Length
1-byte
Flags
Padding Algorithm / Auxiliary Encryption / Compression / Continuation
1-byte
Padding Length
variable
Data
variable
Padding Length

For More Of The

Good Stuff

BarBOF - Thursday evening

Docs
https://darkmail.info/spec

Discuss
https://darkmail.info/forums

Develop
https://darkmail.info/code

FIN