Ladar Levison

Stephen Watt

What is Dark Mail?

What is ~~Dark Mail~~?

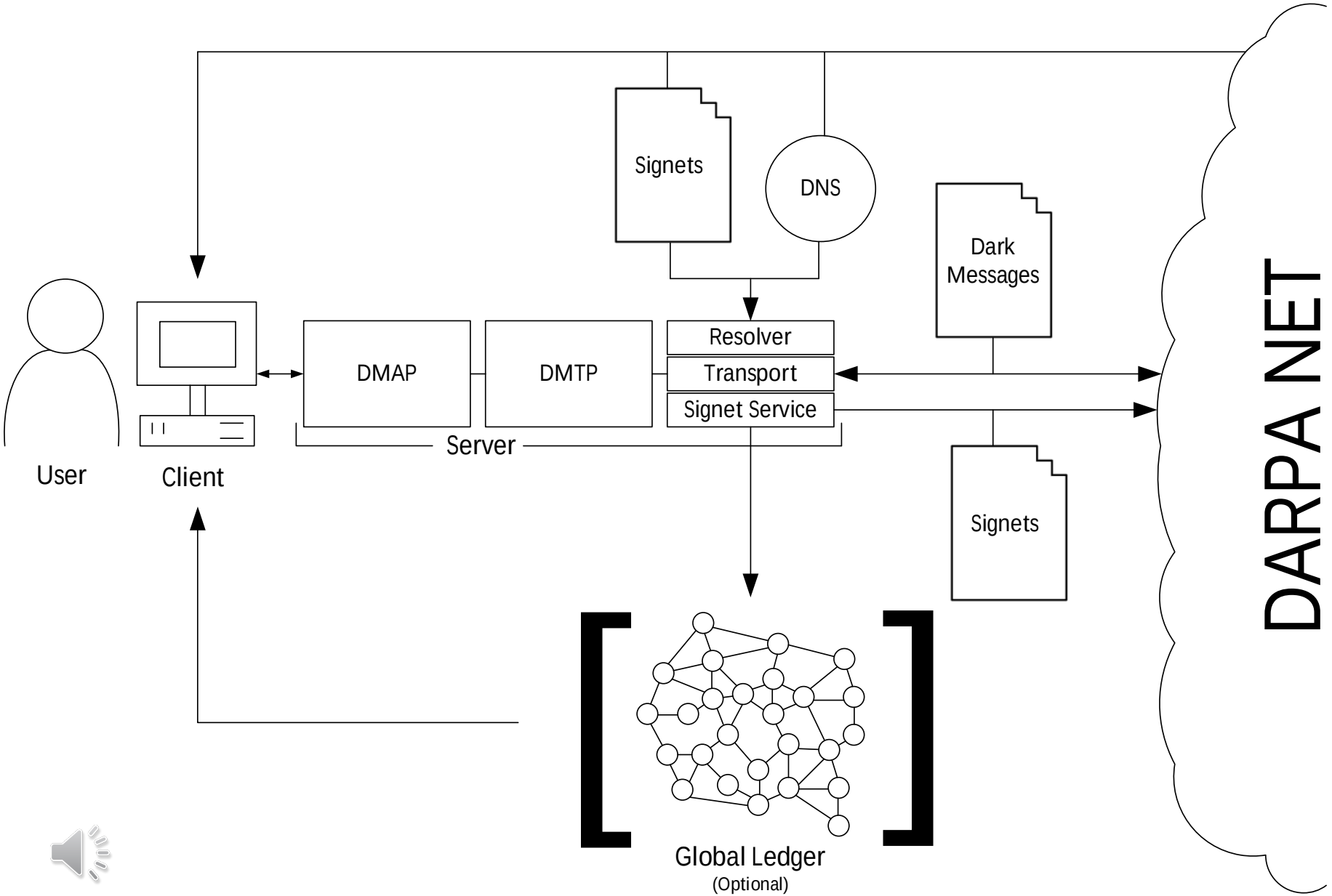
What is DIME?

Did you write down the formula?

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAtO/hOrG2cL+JqA7rIhuqFWz3foroWUnK5mi3NS5js8Yo3Ceh
jHPamUwOrhJNkCV5sj8IRaPiNb55j8/dooOf8dQokt9ZhxaXKabS3dYCwImrHcpP
fj68ienzmqrBTz/E2tMUNe6sX14wBhmCJ/gIDOrForCi7+kKxPsVcQwtN51PWrvI
+g7JPWA0h8fXQnjtWG7bXUABhDcVWniYYW8WhhdydBkh/ODcww+KZGC+amsuHK7B
zTomai33Z2b44j5XyMJvVpbUOicSKwdZU4eBRKuv0ycPBZYzuO1zawsMrWVgCRZo
LsoVqquzFbP6FZo4u4LnMnqu3aBGmSKUkQ50IQIDAQABAoIBAQCrFLHi/Ivjuceg
J1L+sie1EI5HkXI2ksaN6+9nEpDlN/YEjFh85EKKdlbfEqFSLY0PE/hvWJEYfhyU
9Ve8RTajwxYGIbeWOq79jCaP6L47bTBl/5gAZ7N/t71FvjUACOzKd5EBmcZUektw
SQg/YI/EHux2cwvtSm2LaVmRxZCvprCUs84GYd+AoSAJVICxI//YgWaSqqpasK6a
bSmImvYCY0MvXHlw9uw2sSELrD3Cv0sHqOAYntXDdh2RGC0XNc4WkuyBrZ81lDn+
rbvLByl9NuzeWkpO59XRSnrSl7ndzSYT9KWBIRuAgPi8RH7cltlyBoODhN8EFv15
mVg29YItAoGBANd3UWpPGrZD5upqNWcPHttg8OKZVW9arhhE5gL71P4yqvNhw0xi
0nE3xqJjKU+BOcUi3YqWdLlSPx53QQatj/BlbITZFudu59Z7w0puHWu146GZ73pm
329uQ5+WMtseZF7/3Kuh4CUmmYU9Z3kl6XRElTRbCn+oiE+UwygNGWAjAoGBANb5
qzokjn7yP/MMRbeTzQNzoFSzkWotwMFATpiYbSpUDgVhJv7L7mG0gCu7pCtqNxui
oMUNuCz6zNBwc/OFpUOsBkpQ1y9wKOny2Hy78wyFbCoL051KZie62IKJaPurLLrA
P5v21xcZXQ1yYnGwBFvPAJz/5d1MMgfYZHTdCTzrAoGAXk3u6GSvAE8/5iGONgk8
LDCFvef2qMI7qIufUHcAhjGO+O81F125Vaxf1/smvZGFw267IEkx1VrWHXN8lnuo
oEMD+DE8ARddiVap5w3C+r2lX7mMQzp7WL4eAt8uaxEmRR4fa09yV1BJqTNy8mdR
gn3x//RI6A7PemVV9VWmYZkCgYBGvAf3LaglZRhdpKAb82n1xMnwlNU4Fq3h6ILz
+tOQpe+nHXxzQi7Bv16dBTTThDN1yGEV9ZmwUyWpQBcm/caPKb84HLlxRnpv4BQT
ltQ2PoCEpTeP/bb3Q6eR7By7Emu5VyCW9PV5CENx9T0nIz+L5eTRw/Giizu7ERyc
x04O2QKBgC7SlDNmmt5LtUS8Q2JXylSQzjohs6L+IrlYT8AvFNDkb4A9+1cMMpch
LzojFI6qDeMnThLVPPtvfReQm10Q6edcWmEEx4b4r0DiMpr+mfvJXtHlODaQgG/D
Ok0k/HPmWEJXViM4SYCEv3qL1njDrW7++YGYoqEl5saZqoiA930V
-----END RSA PRIVATE KEY-----
```

Dark Internet Mail Environment

DIME *Illustrated*



Why Do We Need It?

- Guilt by Association
- Mass Surveillance (Gotta Love Backbone Slurping)
- Service Provider (PRTT Orders, Search Warrants, NSLs, FISC Warrants)

within the mainstream, but this is a provider that specifically was started in order to have to protect privacy interests more than the average Internet service provider.

THE COURT: I can understand why the system was set up, but I think the government is -- government's clearly entitled to the information that they're seeking, and just because you-all have set up a system that makes that difficult, that doesn't in any way lessen the government's right to receive that information just as they would from any telephone company or any other e-mail source that could provide it easily. Whether it's -- in other words, the difficulty or the ease in obtaining the information doesn't have anything to do with whether or not the government's lawfully entitled to the information.

Goals

- Message Confidentiality
- Author Validation
- Minimize Metadata Exposure
- Automagical Key Management
- Efficient Access from Multiple Clients
- Deployment Flexibility

Get everyone using it! The more people using it, the more valuable it becomes.

THE COURT: All right. Mr. Levison.

MR. LEVISON: Good morning, Your Honor. I'm not sure what order I should make these in, but I would like to request a couple of things by motion.

I'd like to move that all of the nonsensitive portions of the documents that were provided, i.e., everything except the account in question, be unsealed. I believe it's important for the industry and the people to understand what the government is requesting by demanding that I turn over these encryption keys for the entire service.

THE COURT: All right. What do you say to that, Mr. [redacted] Deal with the motions before I --

MR. [redacted] What Mr. Levison is trying to do, Your Honor, is invite industry to come in and litigate as a surrogate for him the issue of whether the encryption keys are part and parcel of the pen register order. And that's one of the reasons we sought the search warrant, to make it clear, whether through the search warrant or pen register order, he is required to provide these keys.

We know he's been in contact with attorneys who also represent industry groups and others who have litigated issues like this in the WikiLeaks context and others. But we would object to unsealing this matter because it's just Mr. --

How far will they go?

Particular Things to be Seized

I. Information to be disclosed by Lavabit, LLC

To the extent that the information described in Attachment A is within the possession, custody, or control of Lavabit, LLC (Lavabit), including any e-mails, records, files, logs, or information that have been deleted but are still available to Lavabit, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Lavabit is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

d. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

For each of the categories above, if Lavabit is able to provide decrypted content, it must do so. If Lavabit is unable to provide decrypted content, Lavabit must provide any and all information necessary to decrypt the content, including, but not limited to public and private keys and algorithms.

II. Information to be seized by the government

[redacted]

b. Evidence of the identities of the users of the account and co-conspirators and others associated with the account and the criminal activities facilitated by the use of the account;

c. Evidence of the location of the users of the account and co-conspirators and others associated with the account, and;

d. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

How will they attack?

Weak Points

- DNS
- Password Strength
- Endpoint Security
- Cryptographic Algorithms
- Implementation Vulnerabilities
- JavaScript Clients
  - For those addicted to Webmail

* Warning: if the world adopts end-to-end cryptography for communications, then it's only a matter of time – hardware will start shipping from the factory with a backdoor.

Let’s Get Back to DIME

Lead by Example


magma


VOLCANO

DIME Management Record

```
[ladar@defcon ~]# host -t txt _dx.lavabit.com
_dx.lavabit.com descriptive text "sig=VGhpcyBpcyBub3QgYSByZWFsIHNp
Z25pbmcga2V5LiBUaGlzIGlzIG5vdCBhIHJlYWwgc2lnbmluZyBrZXku"
```

DIME Management Record

```
[ladar@defcon ~]# host -t txt _dx.lavabit.com
_dx.lavabit.com descriptive text "sig=VGhpcyBpcyBub3QgYSByZWFsIHNp
Z25pbmcga2V5LiBUaGlzIGlzIG5vdCBhIHJlYWwgc2lnbmluZyBrZXku"
```

```
[ladar@defcon ~]# host -t txt _dx.complicated.lavabit.com
_dx.complicated.lavabit.com descriptive text "ver=1 dx=dx.l
avabit.com sig=SSBoYXZlIGJlZW4gZm9yY2VkIHRvIG1ha2UgYSBkaWZm
aWN1bHQgZGVjaXNpb246IHRvIGJlY29tZSBjb21w tls=MmQ1NTAxYmQzM2
Y3YjZlMDYxMTdlNTNjY2YyMTcwMzU2NWYyOWFiNzg2NDJhNzcxZWZmYTQzN
jlmMzI5Mzhi"
```

DIME Management Record

```
[ladar@defcon ~]# host -t txt _dx.lavabit.com
_dx.lavabit.com descriptive text "sig=VGhpcyBpcyBub3QgYSByZWFsIHNp
Z25pbmcga2V5LiBUaGlzIGlzIG5vdCBhIHJlYWwgc2lnbmluZyBrZXku"
```

```
[ladar@defcon ~]# host -t txt _dx.complicated.lavabit.com
_dx.complicated.lavabit.com descriptive text "ver=1 dx=dx.l
avabit.com sig=SSBoYXZlIGJlZW4gZm9yY2VkIHRvIG1ha2UgYSBkaWZm
aWN1bHQgZGVjaXNpb246IHRvIGJlY29tZSBjb21w tls=MmQ1NTAxYmQzM2
Y3YjZlMDYxMTdlNTNjY2YyMTcwMzU2NWYyOWFiNzg2NDJhNzcxZWZmYTQzN
jlmMzI5Mzhi"
```

What is a Signet?

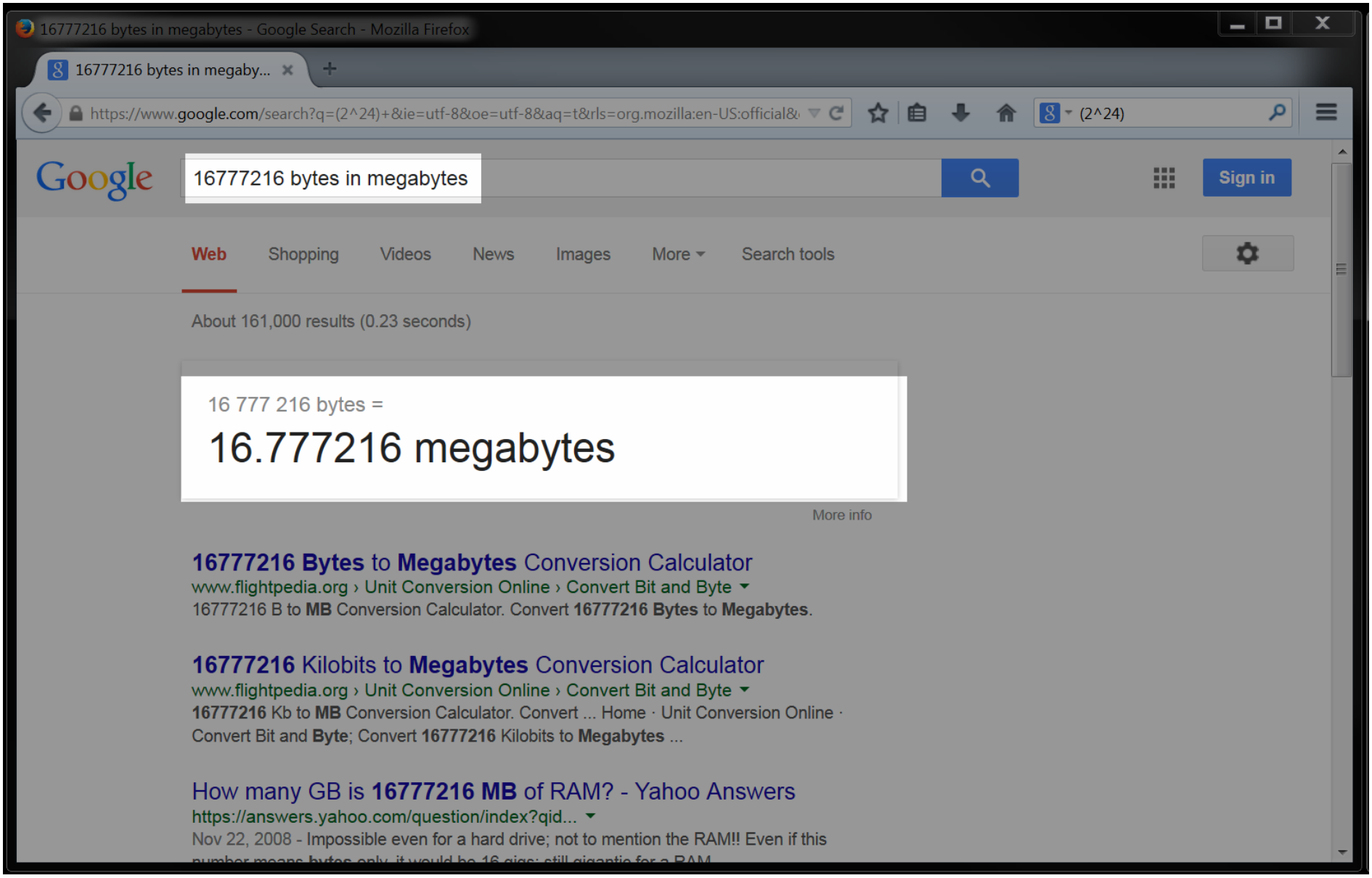
Signet

Header
Byte 1: Signet Format Version Number
Bytes 2-4: Length of the Signet *(minus the 4 byte header)*

Defined Attributes
Byte 1: Attribute Type (Signing key, Encryption Key, Org Signature, Etc.)
Bytes 2-3: Value Length
Bytes 4-X: Value

Undefined Attributes
Byte 1: Indicates Undefined Attribute Type (Value == 255)
Byte 2: Name Length
Bytes 3-N: Name
Bytes (N+1)-(N+3): Value Length
Bytes (N+4)-(N+4+X): Value

* Because the overall length is 3 bytes, the maximum size of a Signet is 16 megabytes.


16777216 bytes in megabytes - Google Search - Mozilla Firefox
16777216 bytes in megaby...
https://www.google.com/search?q=(2^24)+&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&
(2^24)
Google
16777216 bytes in megabytes
Sign in
Web
Shopping
Videos
News
Images
More
Search tools
About 161,000 results (0.23 seconds)
16 777 216 bytes =
16.777216 megabytes
More info
16777216 Bytes to Megabytes Conversion Calculator
www.flightpedia.org › Unit Conversion Online › Convert Bit and Byte
16777216 B to MB Conversion Calculator. Convert 16777216 Bytes to Megabytes.
16777216 Kilobits to Megabytes Conversion Calculator
www.flightpedia.org › Unit Conversion Online › Convert Bit and Byte
16777216 Kb to MB Conversion Calculator. Convert ... Home · Unit Conversion Online · Convert Bit and Byte; Convert 16777216 Kilobits to Megabytes ...
How many GB is 16777216 MB of RAM? - Yahoo Answers
https://answers.yahoo.com/question/index?qid...
Nov 22, 2008 - Impossible even for a hard drive; not to mention the RAM!! Even if this

gravity on earth - Google Search - Mozilla Firefox

gravity on earth - Google ...

https://www.google.com/search?q=gravitational+constant&ie=utf-8&oe=utf-8&aq=t&rls=org.moz

gravitational constant

Google

gravity on earth

Sign in

Web Images Videos Shopping News More Search tools

About 42,500,000 results (0.21 seconds)

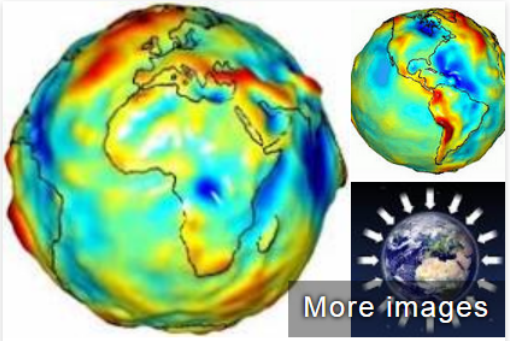
gravity on earth =

$9.80665\ m / s^2$

More info

Gravity of **Earth** - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/**Gravity**_of_**Earth** Wikipedia
The **gravity** of **Earth**, denoted g, refers to the acceleration that the **Earth** imparts to objects on or near its surface. In SI units this acceleration is measured in ...
Variation in gravity and ... - Estimating g from the law of ...

Standard **gravity** - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Standard_**gravity** Wikipedia
Standard **gravity**. From Wikipedia, the free encyclopedia. Jump to: navigation, search. Further information: **Gravity** of **Earth**. The standard acceleration due to ...



Gravity of Earth

The gravity of Earth, denoted g, refers to the acceleration that the Earth imparts to objects on or near its surface. In SI units this acceleration is measured in meters per second squared or equivalently in newtons per kilogram. Wikipedia

gravity on earth - Google Search - Mozilla Firefox

gravity on earth - Google ...

https://www.google.com/search?q=gravitational+constant&ie=utf-8&oe=utf-8&aq=t&rls=org.moz

gravitational constant

Google

gravity on earth

Sign in

Web Images Videos Shopping News More Search tools

About 42,500,000 results (0.21 seconds)

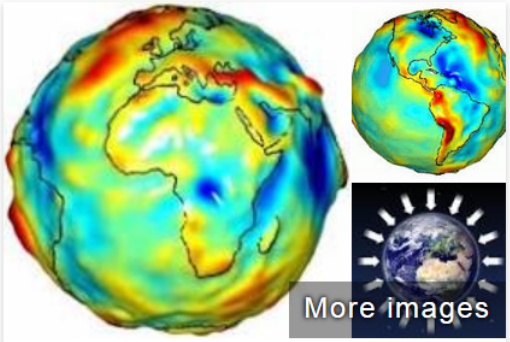
gravity on earth =

$10\ m / s^2$

More info

Gravity of **Earth** - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/**Gravity**_of_**Earth** Wikipedia
The **gravity** of **Earth**, denoted g, refers to the acceleration that the **Earth** imparts to objects on or near its surface. In SI units this acceleration is measured in ...
Variation in gravity and ... - Estimating g from the law of ...

Standard **gravity** - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Standard_**gravity** Wikipedia
Standard **gravity**. From Wikipedia, the free encyclopedia. Jump to: navigation, search. Further information: **Gravity** of **Earth**. The standard acceleration due to ...



Gravity of Earth

The gravity of Earth, denoted g, refers to the acceleration that the Earth imparts to objects on or near its surface. In SI units this acceleration is measured in meters per second squared or equivalently in newtons per kilogram. Wikipedia

Signet Construction

Signet Construction

```
sign=TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVyIGFkaXBpc2NpbmcgZWxpdCBwb3N1ZXJlLiA
encrypt=VEc5eVpXMGdhWEJ6ZFcwZ1pHOXNiM0lnYzJsMElHRnRaWFFzSUdOdmJuTmxZM1JsZEhWeUlHRmthWEJwYzJOYS4

user=VkVjNWVWcFhNR2RoV0VKNlpGY3daMXBIT1hOaU0wbG5ZekpzTUVsSFJuUmFXRkZ6U1VkT2RtSnVUbXhaTTFKcwa
organization=VmtWak5XVldjRmhOUjJSb1YwVktObHBHWTNkYU1YQklUMWhPYVUwd2JHNVpla3B6VFVWc1NGSnVVbUZYUmtaYQa
```

Signet Construction

sign=TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVyIGFkaXBpc2NpbmcgZWxpdCBwb3N1ZXJlLiA
encrypt=VEc5eVpXMGdhWEJ6ZFcwZ1pHOXNiM0lnYzJsMElHRnRaWFFzSUdOdmJuTmxZM1JsZEhWeUlHRmthWEJwYzJOYS4
custody=dXVIdGUxN3Mxd1JsdUxlNEg2Q2h0SnVUMXlPL0FxVDhIQWY0eGhMckRNWjNpLzhBS0V3TGhkM2htQXNTc3QwQwM

user=VkVjNWVWcFhNR2RoV0VKNlpGY3daMXBIT1hOaU0wbG5ZekpzTUVsSFJuUmFXRkZ6U1VkT2RtSnVUbXhaTTFKcwa
organization=VmtWak5XVldjRmhOUjJSb1YwVktObHBHWTNkYU1YQklUMWhPYVUwd2JHNVpla3B6VFVWc1NGSnVVbUZYUmtaYQa

Signet Construction

sign=TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVyIGFkaXBpc2NpbmcgZWxpdCBwb3N1ZXJlLiA
encrypt=VEc5eVpXMGdhWEJ6ZFcwZ1pHOXNiM0lnYzJsMElHRnRaWFFzSUdOdmJuTmxZM1JsZEhWeUlHRmthWEJwYzJOYS4
custody=dXVIdGUxN3Mxd1JsdUxlNEg2Q2h0SnVUMXlPL0FxVDhIQWY0eGhMckRNWjNpLzhBS0V3TGhkM2htQXNTc3QwQwM

user=VkVjNWVWcFhNR2RoV0VKNlpGY3daMXBIT1hOaU0wbG5ZekpzTUVsSFJuUmFXRkZ6U1VkT2RtSnVUbXhaTTFKcwa
organization=VmtWak5XVldjRmhOUjJSb1YwVktObHBHWTNkYU1YQklUMWhPYVUwd2JHNVpla3B6VFVWc1NGSnVVbUZYUmtaYQa

name=Glenn Greenwald

photo=**/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEAAkGBwgHBgkIBwgKCgkLDRYPDQwMDRsUFRAWIB0iIiAdHx8kKDQsJCYxJx8fLT0tMTU3Ojo6Iys/RD84QzQ5OjcBCgoKDQwNGg8PGjclHyU3**
Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3N//AABEIAHoAbgMBIgACEQEDEQH/xAAcAAABBAMBAAAAAAAAAAAAAAAABAUGBwECAwj/xAA9EAABAwIEAwYC
BwYHAQAAAAABAAIDBBEFEiExBhNBByJRYXGBMpEUI1KhscHwJDNCgtHhFTREcqKy8Qj/xAAZAQADAQEBAAAAAAAAAAAAAAAAAQIEAwX/xAAeEQADAQEAAwEBAQAAAAAAAAAAAQIRAxIhMQQTQf/a
AAwDAQACEQMRAD8AvFCEIAEISHGsVo8Fw6WvxGblU8Q1IaXEnoABqT6IAXFRHHO0jhbBXSRz4lHPOxpPJpfrTfwuNAfUhUdxz2lYzxJNLT0tRJS4bmLWxxXZzRfQu1v7XsobFBI++g11spbGlpfM
/bngzXM5GE4g9pPeLjG2w8u8blOWGdsvC9ZLFHUNraIyG2eaIFjT5lpNvWy8+spH9AfVbijJdYC7lPkX/NnrfDcXw/FII5sPq4J2SXymN4O2+nkly8f4ZVVeD4jDW0croaiFwex43uP7Ej3XofgL
tDouJwykqR9FxM3PKt3JANe6fyNjuqVaS5wnKEIVEghCEACEIQAKl/8A6IxJ2TCsIbnIlzzvGezdCALt6nU6+ul9RdCoTt/ueMcGa1lv2Qkutv3zp7W+9J/BytZA8JwB9WW5+6PvUppeDi7Ly5A0
DqRr7JTg0TWZS4bqWUneAAsFkro2z1o4QkMdPwhShn10j5n2tc6fgudZwrEyNxjJzEWAOymNmhouUnqWh4sPmubbOiifmFVY5gz6eLnaG56DzW3Bz5YOI8NdT1Ap5eezJIQSM17AHyd8J8nFTPH6
ZslDIy2wUBEcoJbTB3POkQbvm6W872XTnWox9+amvR6tGoWVhuoWVsMAIQhAAhCEACp/t6w0uq8AxIXytfJTuFvEZhr/ACuVwKqu2vF3CngwcUmbvx1H0gn4DdzbAW8Lg69VNfC+abr0Q/C3AtYS
eildIzQEOFvNV9Rx0sVO59a2qmexoc5sTrWT7Qz/AEeJk1NzmwyNuGSyBxte1wsjnD1p6EzzNZe7gAN7pvnxega8x/SYi4bgOW9SwS0bHBxJcNUwVLOTy3w4RBUEuLTe+YHofK/ioXstvBzllgq4
yI3g30UUw2hfHxdhlNYkmvgGg6cxtzb0upJFS82V5bByS07s1a70SeGgkPEfP+HJFmD7ddvmlLxnHpPmXkFlM/ClTLVYJA6dxdKy7HOJve39rJ4XoJ6tPLqfFtMEIQmSCEIQAKsO1mH9sikfbI6m
7oPUtff8wrPUV7QsFfi2CmSCMvqKYlzWtFy5p0cB9x9lHRbJ24UptaVdhlIx45thcjXoumLOLYmMNrXGy54NI4R8t2hGhB6JXiMbbMvqM4zeQWNfT1Vg8QXNNF5pY2CNwznf0SZ8kDaWJrJAT0y+
KXQsPJAdfbql8Kr2J5QBoEkygl9gc9hl8tUsnFuqVcP4VJicr7ECFrgJXX1t4AeKUzr9HKrUe2S7heD6PgsAIsX3efc6fdZOy1jY2NjWNADWiwA6BbL0EsWHk3XlTYIQhMkEIQgAWLXWUIApvi2i
dhXGNYMtoqo/SI7DfN8X/LMm6pqG52tncG5h1VmdoOEQ1+BS1hIZUUDHTRv8gLuafIgfMBVbTyisyk2uBp5LL0nxrT0vzdPKcf8Ag9UNRR04s2eI6C2U3KXsrWSG0biR9qxsm+kZObWbdvkEtfIQ
Ax2lui5s01iRvO/TdSHgGVpfWxEjMcjgPEa3/JRN7i4kBPfDbZaSQ1rdh3Wj7Q6rpyh+Rj70nDbLCQucE0czA+N4cCOnRdFqMAIQhAAhC5TzxU8TpZ5WRxt3c42AQB1XKoqIaaIyzysijbu97rAK
LYrxlG28WGRc123NkFmj0G5+5Reslqqxxq K6d8h6F50HoOnsrUNi0f8AiXi+lloamko6c1DZIyx0kndbYi2g3PvZVbyZcPna8X5Tvgd+R81IK63Kys8LlKKCnjqKcxysDmO3aeqv+SpYVHZ83oig
xQta0Nve3glMb3yagWvuSuFZhc2HgSxuD4L7uIDh5FSLAsIdURsnq25WEXbEeo8/6LMvz15Zhuf6I8PJsMHwl9VaWS7YfXV368VIzE1jAxgAAFgB0XdjQxlgNlq/RuY/JalzUrEYL6Vb1iRrMj8z
CWu+002IS+DFKqGwlAnZ47OSQMaDcDzK3LQBcbHok4ROj5SV1PVaRvs/7DtHJUoqWNcbjQjY7WSuHEqqAZXWlb0Lt/mocYPRZjuNU+DUoll78r9IogdXn8h4lV/X19djNQHVTrj+CJg7rPb81yqJ
JcVxiWepcXF8jgBf4WNdYAeATzhtK2OBsrhqRp6K5jCaYjhpI6aPmzDUC6RVAkmc1z/4j3WpxqS+qnyxi7Grk2AuqtTowbroI4NoQ4PB3LUkoQY3lv2dE6vc98hgpm5nu0J8Fo+hNJK0FxcLXLjr
r+vxQgIV2gz1EmKQQSNDaZsV423+J97ONvEaD/1S7szxSSfDpaCocXCncBC925aR8PtZRTtDmidU0MMZ+ujaXZ+oaTYf9Sl3AAe6Wrjhdlnfy3i/S19fvCYFp26LjN0tsFmGXNES7R40cPArGrrI
A0Hkt26tstG919jsV0buQpATuFnWO11kkg6E2stqlv1ebwK3YwFoJvqEYBCqS4kgcN5Yj83Ocf6KSPYXRtgi0baxKj9F/oP9jPwKk0Wya+gxLPyqaPI3Sw3TdFzal/KptLm7nla4s45wLm107YM0
CLQBAHampIMPguR3urjuSm6qe+rlPLb3WjQdPdLMUJ5zRc2tsuNNph9Q4b5Tr7J/BFScSVjKzH6mRpzRxEQtGY65Ra/zunzgCoMXE1MwuuHte17s1wRluLe4H6ChtJuT1yO/AqT8HAf4xhLrDMZ3
i/8AKEwLhd3hmAsSst0CydggKRmHt7gPVZvaz/mtpPhCwP3fsgDNQAad9vBYjeAxo8kO/wAqfRaP/ct9vwVCP//Z

organization=WjNpLzhBS0V3TGhkM2htQXNTc3QwQ3lkZ2dLUm1IdDdnUFZadmF6L210cFBoQ3dQM2ZzZ0ROUUFhZDl2QllqZQ6

Signet Construction

sign=TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVyIGFkaXBpc2NpbmcgZWxpdCBwb3N1ZXJlLiA
encrypt=VEc5eVpXMGdhWEJ6ZFcwZ1pHOXNiM0lnYzJsMElHRnRaWFFzSUdOdmJuTmxZM1JsZEhWeUlHRmthWEJwYzJOYS4
custody=dXVIdGUxN3Mxd1JsdUxlNEg2Q2h0SnVUMXlPL0FxVDhIQWY0eGhMckRNWjNpLzhBS0V3TGhkM2htQXNTc3QwQwM

user=VkVjNWVWcFhNR2RoV0VKNlpGY3daMXBIT1hOaU0wbG5ZekpzTUVsSFJuUmFXRkZ6U1VkT2RtSnVUbXhaTTFKcwa
organization=VmtWak5XVldjRmhOUjJSb1YwVktObHBHWTNkYU1YQklUMWhPYVUwd2JHNVpla3B6VFVWc1NGSnVVbUZYUmtaYQa

name=Glenn Greenwald
photo=/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEAAkGBwgHBgkIBwgKCgkLDRYPDQwMDRsUFRAWIB0iIiAdHx8kKDQsJCYxJx8fLT0tMTU3Ojo6Iys/RD84QzQ5OjcBCgoKDQwNGg8PGjclHyU3
Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3N//AABEIAHoAbgMBIgACEQEDEQH/xAAcAAABBAMBAAAAAAAAAAAAAAAABAUGBwECAwj/xAA9EAABAwIEAwYC
BwYHAQAAAAABAAIDBBEFEiExBhNBByJRYXGBMpEUI1KhscHwJDNCgtHhFTREcqKy8Qj/xAAZAQADAQEBAAAAAAAAAAAAAAAAAQIEAwX/xAAeEQADAQEAAwEBAQAAAAAAAAAAAQIRAxIhMQQTQf/a
AAwDAQACEQMRAD8AvFCEIAEISHGsVo8Fw6WvxGblU8Q1IaXEnoABqT6IAXFRHHO0jhbBXSRz4lHPOxpPJpfrTfwuNAfUhUdxz2lYzxJNLT0tRJS4bmLWxxXZzRfQu1v7XsobFBI++g11spbGlpfM
/bngzXM5GE4g9pPeLjG2w8u8blOWGdsvC9ZLFHUNraIyG2eaIFjT5lpNvWy8+spH9AfVbijJdYC7lPkX/NnrfDcXw/FII5sPq4J2SXymN4O2+nkly8f4ZVVeD4jDW0croaiFwex43uP7Ej3XofgL
tDouJwykqR9FxM3PKt3JANe6fyNjuqVaS5wnKEIVEghCEACEIQAKl/8A6IxJ2TCsIbnIlzzvGezdCALt6nU6+ul9RdCoTt/ueMcGa1lv2Qkutv3zp7W+9J/BytZA8JwB9WW5+6PvUppeDi7Ly5A0
DqRr7JTg0TWZS4bqWUneAAsFkro2z1o4QkMdPwhShn10j5n2tc6fgudZwrEyNxjJzEWAOymNmhouUnqWh4sPmubbOiifmFVY5gz6eLnaG56DzW3Bz5YOI8NdT1Ap5eezJIQSM17AHyd8J8nFTPH6
ZslDIy2wUBEcoJbTB3POkQbvm6W872XTnWox9+amvR6tGoWVhuoWVsMAIQhAAhCEACp/t6w0uq8AxIXytfJTuFvEZhr/ACuVwKqu2vF3CngwcUmbvx1H0gn4DdzbAW8Lg69VNfC+abr0Q/C3AtYS
eildIzQEOFvNV9Rx0sVO59a2qmexoc5sTrWT7Qz/AEeJk1NzmwyNuGSyBxte1wsjnD1p6EzzNZe7gAN7pvnxega8x/SYi4bgOW9SwS0bHBxJcNUwVLOTy3w4RBUEuLTe+YHofK/ioXstvBzllgq4
yI3g30UUw2hfHxdhlNYkmvgGg6cxtzb0upJFS82V5bByS07s1a70SeGgkPEfP+HJFmD7ddvmlLxnHpPmXkFlM/ClTLVYJA6dxdKy7HOJve39rJ4XoJ6tPLqfFtMEIQmSCEIQAKsO1mH9sikfbI6m
7oPUtff8wrPUV7QsFfi2CmSCMvqKYlzWtFy5p0cB9x9lHRbJ24UptaVdhlIx45thcjXoumLOLYmMNrXGy54NI4R8t2hGhB6JXiMbbMvqM4zeQWNfT1Vg8QXNNF5pY2CNwznf0SZ8kDaWJrJAT0y+
KXQsPJAdfbql8Kr2J5QBoEkygl9gc9hl8tUsnFuqVcP4VJicr7ECFrgJXX1t4AeKUzr9HKrUe2S7heD6PgsAIsX3efc6fdZOy1jY2NjWNADWiwA6BbLOEsWHk3XlTYIQhMkEIQgAWLXWUIApvi2i
dhXGNYMtoqo/SI7DfN8X/LMm6pqG52tncG5h1VmdoOEQ1+BS1hIZUUDHTRv8gLuafIgfMBVbTyisyk2uBp5LL0nxrT0vzdPKcf8Ag9UNRR04s2eI6C2U3KXsrWSG0biR9qxsm+kZObWbdvkEtfIQ
Ax2lui5s01iRvO/TdSHgGVpfWxEjMcjgPEa3/JRN7i4kBPfDbZaSQ1rdh3Wj7Q6rpyh+Rj70nDbLCQucE0czA+N4cCOnRdFqMAIQhAAhC5TzxU8TpZ5WRxt3c42AQB1XKoqIaaIyzysijbu97rAK
LYrxlG28WGRc123NkFmj0G5+5Reslqqxxq K6d8h6F50HoOnsrUNi0f8AiXi+lloamko6c1DZIyx0kndbYi2g3PvZVbyZcPna8X5Tvgd+R81IK63Kys8LlKKCnjqKcxysDmO3aeqv+SpYVHZ83oig
xQta0Nve3glMb3yagWvuSuFZhc2HgSxuD4L7uIDh5FSLAsIdURsnq25WEXbEeo8/6LMvz15Zhuf6I8PJsMHwl9VaWS7YfXV368VIzE1jAxgAAFgB0XdjQxlgNlq/RuY/JalzUrEYL6Vb1iRrMj8z
CWu+002IS+DFKqGwlAnZ47OSQMaDcDzK3LQBcbHok4ROj5SV1PVaRvs/7DtHJUoqWNcbjQjY7WSuHEqqAZXWlb0Lt/mocYPRZjuNU+DUoll78r9IogdXn8h4lV/X19djNQHVTrj+CJg7rPb81yqJ
JcVxiWepcXF8jgBf4WNdYAeATzhtK2OBsrhqRp6K5jCaYjhpI6aPmzDUC6RVAkmc1z/4j3WpxqS+qnyxi7Grk2AuqtTowbroI4NoQ4PB3LUkoQY3lv2dE6vc98hgpm5nu0J8Fo+hNJK0FxcLXLjr
r+vxQgIV2gz1EmKQQSNDaZsV423+J97ONvEaD/1S7szxSSfDpaCocXCncBC925aR8PtZRTtDmidU0MMZ+ujaXZ+oaTYf9Sl3AAe6Wrjhdlnfy3i/S19fvCYFp26LjN0tsFmGXNES7R40cPArGrrI
A0Hkt26tstG919jsV0buQpATuFnWO11kkg6E2stqlv1ebwK3YwFoJvqEYBCqS4kgcN5Yj83Ocf6KSPYXRtgi0baxKj9F/oP9jPwKk0Wya+gxLPyqaPI3Sw3TdFzal/KptLm7nla4s45wLm107YM0
CLQBAHampIMPguR3urjuSm6qe+rlPLb3WjQdPdLMUJ5zRc2tsuNNph9Q4b5Tr7J/BFScSVjKzH6mRpzRxEQtGY65Ra/zunzgCoMXE1MwuuHte17s1wRluLe4H6ChtJuT1yO/AqT8HAf4xhLrDMZ3
i/8AKEwLhd3hmAsSst0CydggKRmHt7gPVZvaz/mtpPhCwP3fsgDNQAad9vBYjeAxo8kO/wAqfRaP/ct9vwVCP//Z

organization=WjNpLzhBS0V3TGhkM2htQXNTc3QwQ3lkZ2dLUm1IdDdnUFZadmF6L210cFBoQ3dQM2ZzZ0ROUUFhZDl2Q1lqZQ6

Signet Construction

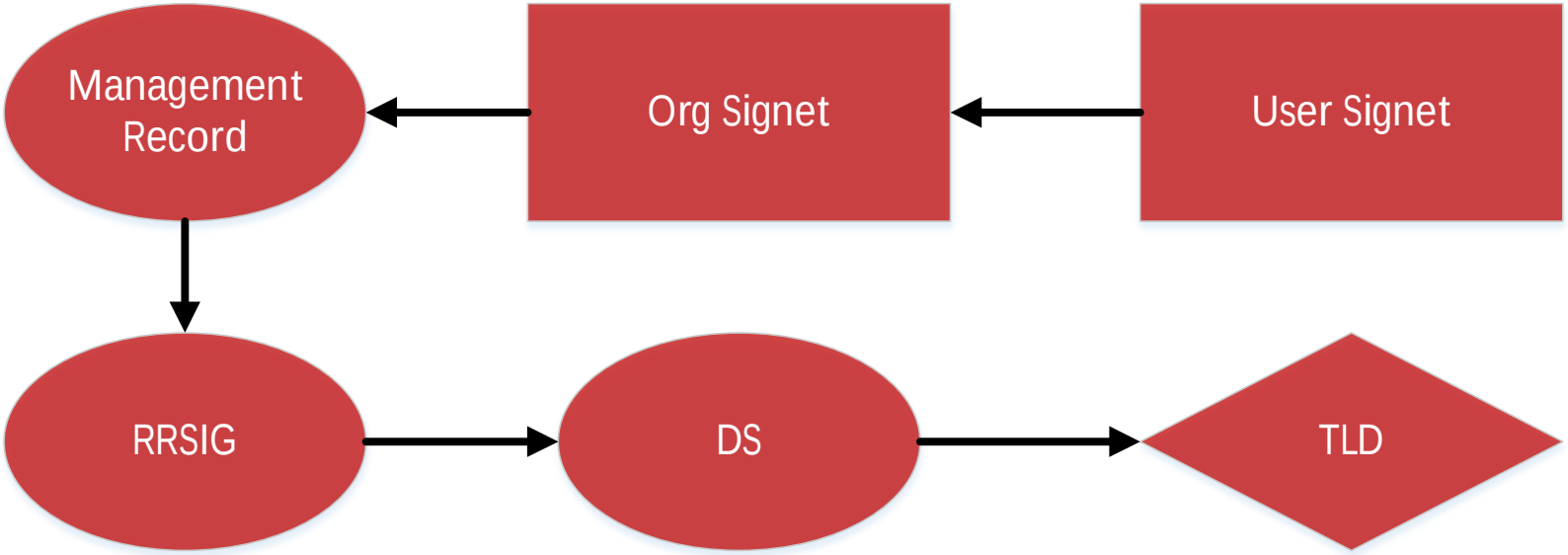

```
sign=TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVyIGFkaXBpc2NpbmcgZWxpdCBwb3N1ZXJlLiA
encrypt=VEc5eVpXMGdhWEJ6ZFcwZ1pHOXNiM0lnYzJsMElHRnRaWFFzSUdOdmJuTmxZM1JsZEhWeUlHRmthWEJwYzJOYS4
custody=dXVIdGUxN3Mxd1JsdUxlNEg2Q2h0SnVUMXlPL0FxVDhIQWY0eGhMckRNWjNpLzhBS0V3TGhkM2htQXNTc3QwQwM

user=VkVjNWVWcFhNR2RoV0VKNlpGY3daMXBIT1hOaU0wbG5ZekpzTUVsSFJuUmFXRkZ6U1VkT2RtSnVUbXhaTTFKcwa
organization=VmtWak5XVldjRmhOUjJSb1YwVktObHBHWTNkYU1YQklUMWhPYVUwd2JHNVpla3B6VFVWc1NGSnVVbUZYUmtaYQa

name=Glenn Greenwald
photo=/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEAAkGBwgHBgkIBwgKCgkLDRYPDQwMDRsUFRAWIB0iIiAdHx8kKDQsJCYxJx8fLT0tMTU3Ojo6Iys/RD84QzQ5OjcBCgoKDQwNGg8PGjclHyU3
Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3N//AABEIAHoAbgMBIgACEQEDEQH/xAAcAAABBAMBAAAAAAAAAAAAAAAABAUGBwECAwj/xAA9EAABAwIEAwYC
BwYHAQAAAAABAAIDBBEFEiExBhNBByJRYXGBMpEUI1KhscHwJDNCgtHhFTREcqKy8Qj/xAAZAQADAQEBAAAAAAAAAAAAAAAAAQIEAwX/xAAeEQADAQEAAwEBAQAAAAAAAAAAAQIRAxIhMQQTQf/a
AAwDAQACEQMRAD8AvFCEIAEISHGsVo8Fw6WvxGblU8Q1IaXEnoABqT6IAXFRHHO0jhbBXSRz4lHPOxpPJpfrTfwuNAfUhUdxz2lYzxJNLT0tRJS4bmLWxxXZzRfQu1v7XsobFBI++g11spbGlpfM
/bngzXM5GE4g9pPeLjG2w8u8blOWGdsvC9ZLFHUNraIyG2eaIFjT5lpNvWy8+spH9AfVbijJdYC7lPkX/NnrfDcXw/FII5sPq4J2SXymN4O2+nkly8f4ZVVeD4jDW0croaiFwex43uP7Ej3XofgL
tDouJwykqR9FxM3PKt3JANe6fyNjuqVaS5wnKEIVEghCEACEIQAKl/8A6IxJ2TCsIbnIlzzvGezdCALt6nU6+ul9RdCoTt/ueMcGa1lv2Qkutv3zp7W+9J/BytZA8JwB9WW5+6PvUppeDi7Ly5A0
DqRr7JTg0TWZS4bqWUneAAsFkro2z1o4QkMdPwhShn10j5n2tc6fgudZwrEyNxjJzEWAOymNmhouUnqWh4sPmubbOiifmFVY5gz6eLnaG56DzW3Bz5YOI8NdT1Ap5eezJIQSM17AHyd8J8nFTPH6
ZslDIy2wUBEcoJbTB3POkQbvm6W872XTnWox9+amvR6tGoWVhuoWVsMAIQhAAhCEACp/t6w0uq8AxIXytfJTuFvEZhr/ACuVwKqu2vF3CngwcUmbvx1H0gn4DdzbAW8Lg69VNfC+abr0Q/C3AtYS
eildIzQEOFvNV9Rx0sVO59a2qmexoc5sTrWT7Qz/AEeJk1NzmwyNuGSyBxte1wsjnD1p6EzzNZe7gAN7pvnxega8x/SYi4bgOW9SwS0bHBxJcNUwVLOTy3w4RBUEuLTe+YHofK/ioXstvBzllgq4
yI3g30UUw2hfHxdhlNYkmvgGg6cxtzb0upJFS82V5bByS07s1a70SeGgkPEfP+HJFmD7ddvmlLxnHpPmXkFlM/ClTLVYJA6dxdKy7HOJve39rJ4XoJ6tPLqfFtMEIQmSCEIQAKsO1mH9sikfbI6m
7oPUtff8wrPUV7QsFfi2CmSCMvqKYlzWtFy5p0cB9x9lHRbJ24UptaVdhlIx45thcjXoumLOLYmMNrXGy54NI4R8t2hGhB6JXiMbbMvqM4zeQWNfT1Vg8QXNNF5pY2CNwznf0SZ8kDaWJrJAT0y+
KXQsPJAdfbql8Kr2J5QBoEkygl9gc9hl8tUsnFuqVcP4VJicr7ECFrgJXX1t4AeKUzr9HKrUe2S7heD6PgsAIsX3efc6fdZOy1jY2NjWNADWiwA6BbL0EsWHk3XlTYIQhMkEIQgAWLXWUIApvi2i
dhXGNYMtoqo/SI7DfN8X/LMm6pqG52tncG5h1VmdoOEQ1+BS1hIZUUDHTRv8gLuafIgfMBVbTyisyk2uBp5LL0nxrT0vzdPKcf8Ag9UNRR04s2eI6C2U3KXsrWSG0biR9qxsm+kZObWbdvkEtfIQ
Ax2lui5s01iRvO/TdSHgGVpfWxEjMcjgPEa3/JRN7i4kBPfDbZaSQ1rdh3Wj7Q6rpyh+Rj70nDbLCQucE0czA+N4cCOnRdFqMAIQhAAhC5TzxU8TpZ5WRxt3c42AQB1XKoqIaaIyzysijbu97rAK
LYrxlG28WGRc123NkFmj0G5+5ReslqqxxqK6d8h6F50HoOnsrUNi0f8AiXi+lloamko6c1DZIyx0kndbYi2g3PvZVbyZcPna8X5Tvgd+R81IK63Kys8LlKKCnjqKcxysDmO3aeqv+SpYVHZ83oig
xQta0Nve3glMb3yagWvuSuFZhc2HgSxuD4L7uIDh5FSLAsIdURsnq25WEXbEeo8/6LMvz15Zhuf6I8PJsMHwl9VaWS7YfXV368VIzE1jAxgAAFgB0XdjQxlgNlq/RuY/JalzUrEYL6Vb1iRrMj8z
CWu+002IS+DFKqGwlAnZ47OSQMaDcDzK3LQBcbHok4ROj5SV1PVaRvs/7DtHJUoqWNcbjQjY7WSuHEqqAZXWlb0Lt/mocYPRZjuNU+DUoll78r9IogdXn8h4lV/X19djNQHVTrj+CJg7rPb81yqJ
JcVxiWepcXF8jgBf4WNdYAeATzhtK2OBsrhqRp6K5jCaYjhpI6aPmzDUC6RVAkmc1z/4j3WpxqS+qnyxi7Grk2AuqtTowbroI4NoQ4PB3LUkoQY3lv2dE6vc98hgpm5nu0J8Fo+hNJK0FxcLXLjr
r+vxQgIV2gz1EmKQQSNDaZsV423+J97ONvEaD/1S7szxSSfDpaCocXCncBC925aR8PtZRTtDmidU0MMZ+ujaXZ+oaTYf9Sl3AAe6Wrjhdlnfy3i/S19fvCYFp26LjN0tsFmGXNES7R40cPArGrrI
A0Hkt26tstG919jsV0buQpATuFnWO11kkg6E2stqlv1ebwK3YwFoJvqEYBCqS4kgcN5Yj83Ocf6KSPYXRtgi0baxKj9F/oP9jPwKk0Wya+gxLPyqaPI3Sw3TdFzal/KptLm7nla4s45wLm107YM0
CLQBAHampIMPguR3urjuSm6qe+rlPLb3WjQdPdLMUJ5zRc2tsuNNph9Q4b5Tr7J/BFScSVjKzH6mRpzRxEQtGY65Ra/zunzgCoMXE1MwuuHte17s1wRluLe4H6ChtJuT1yO/AqT8HAf4xhLrDMZ3
i/8AKEwLhd3hmAsSst0CydggKRmHt7gPVZvaz/mtpPhCwP3fsgDNQAad9vBYjeAxo8kO/wAqfRaP/ct9vwVCP//Z
```


bitcoin=19gy9ifMJuHoRbVpXBgtf6NTAT6PiDb8SQ
motto=It is the duty of every patriot to protect his country from its government.


```
organization=aGtNMmh0UVhOVGMzUXdRM2xrWjJkTFVtMUlkRGRuVUZaYWRtRjZMMjEwY0ZCb1EzZFFNMlp6WjBST1VVRmhaRAF
```

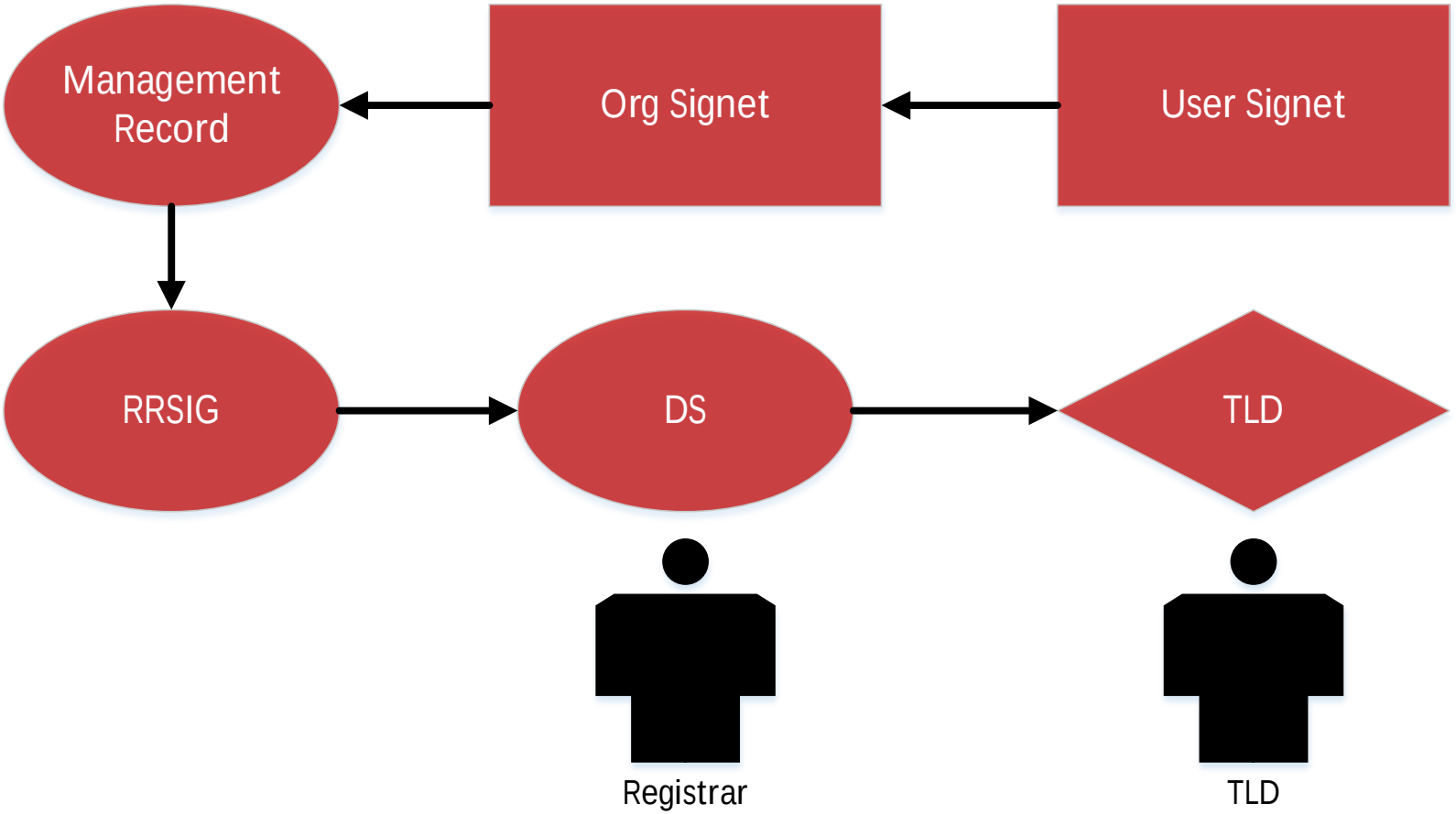
Trust Model

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



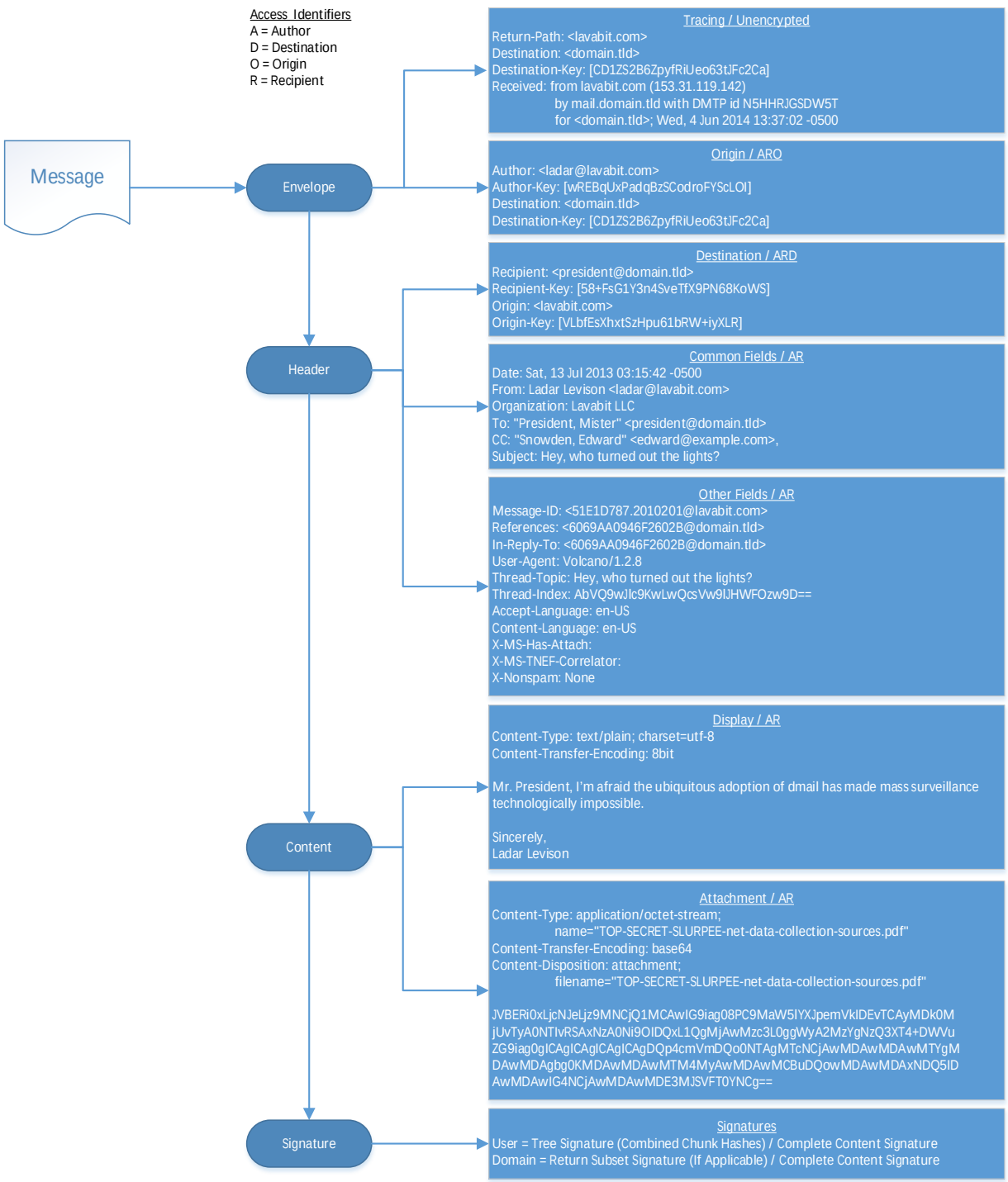
Trust Model

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

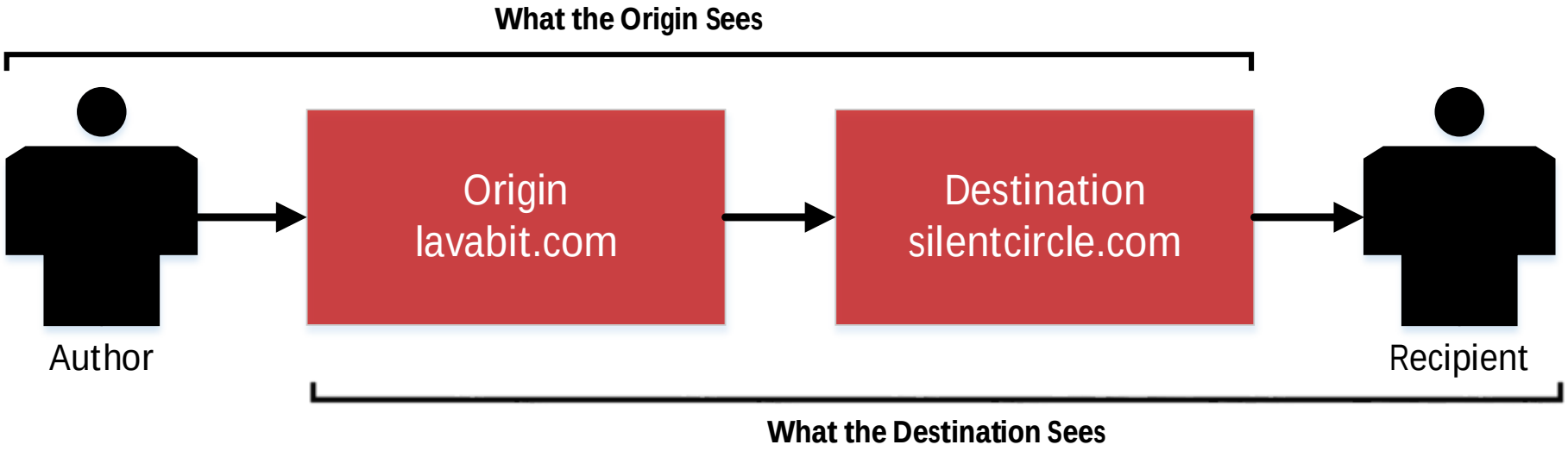


* Trust no one. You'll live longer.

Princess


Access Identifiers
A = Author
D = Destination
O = Origin
R = Recipient
Message
Envelope
Header
Content
Signature
Tracing / Unencrypted
Return-Path: <lavabit.com>
Destination: <domain.tld>
Destination-Key: [CD1ZS2B6ZpyfRiUeo63tJFc2Ca]
Received: from lavabit.com (153.31.119.142)
by mail.domain.tld with DMTP id N5HHRJGSDW5T
for <domain.tld>; Wed, 4 Jun 2014 13:37:02 -0500
Origin / ARO
Author: <ladar@lavabit.com>
Author-Key: [wREBqUxPadqBzSCodroFYScLOI]
Destination: <domain.tld>
Destination-Key: [CD1ZS2B6ZpyfRiUeo63tJFc2Ca]
Destination / ARD
Recipient: <president@domain.tld>
Recipient-Key: [58+FsG1Y3n4SveTfX9PN68KoWS]
Origin: <lavabit.com>
Origin-Key: [VLbfEsXhxtSzHpu61bRW+iyXLR]
Common Fields / AR
Date: Sat, 13 Jul 2013 03:15:42 -0500
From: Ladar Levison <ladar@lavabit.com>
Organization: Lavabit LLC
To: "President, Mister" <president@domain.tld>
CC: "Snowden, Edward" <edward@example.com>,
Subject: Hey, who turned out the lights?
Other Fields / AR
Message-ID: <51E1D787.2010201@lavabit.com>
References: <6069AA0946F2602B@domain.tld>
In-Reply-To: <6069AA0946F2602B@domain.tld>
User-Agent: Volcano/1.2.8
Thread-Topic: Hey, who turned out the lights?
Thread-Index: AbVQ9wJlc9KwLwQcsVw9lJHWFOzw9D==
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
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 made mass surveillance technologically impossible.
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"
JVBERi0xLjcNJeLjz9MNCjQ1MCAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyMDk0M
jUvTyA0NTIvRSAxNzA0Ni9OIDQxL1QgMjAwMzc3L0ggWyA2MzYgNzQ3XT4+DWVu
ZG9iag0gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
DQp4cmVmDQo0NTAgMTcNCjAwMDAwMDAwMTYgM
DAwMDAgbg0KMDAwMDAwMTM4MyAwMDAwMCBuDQowMDAwMDAxNDQ5ID
AwMDAwIG4NCjAwMDAwMDE3MjSVFT0YNCg==
Signatures
User = Tree Signature (Combined Chunk Hashes) / Complete Content Signature
Domain = Return Subset Signature (If Applicable) / Complete Content Signature

Pseudo Onion



Fin