Privacy and Security

Purpose of the session

A conversation around where we think the Encryption issue leads to.

Share thoughts about the issues.

20 minutes introduction 20 minutes of conversation.

Background and ISOC status

1994 Clipper

1996 RFC1984

June 2013 - NSA breach

May 2014 - RFC7258

September 2014 - IOS 8

Jan-Dec 2015 - Letsencrypt got viable

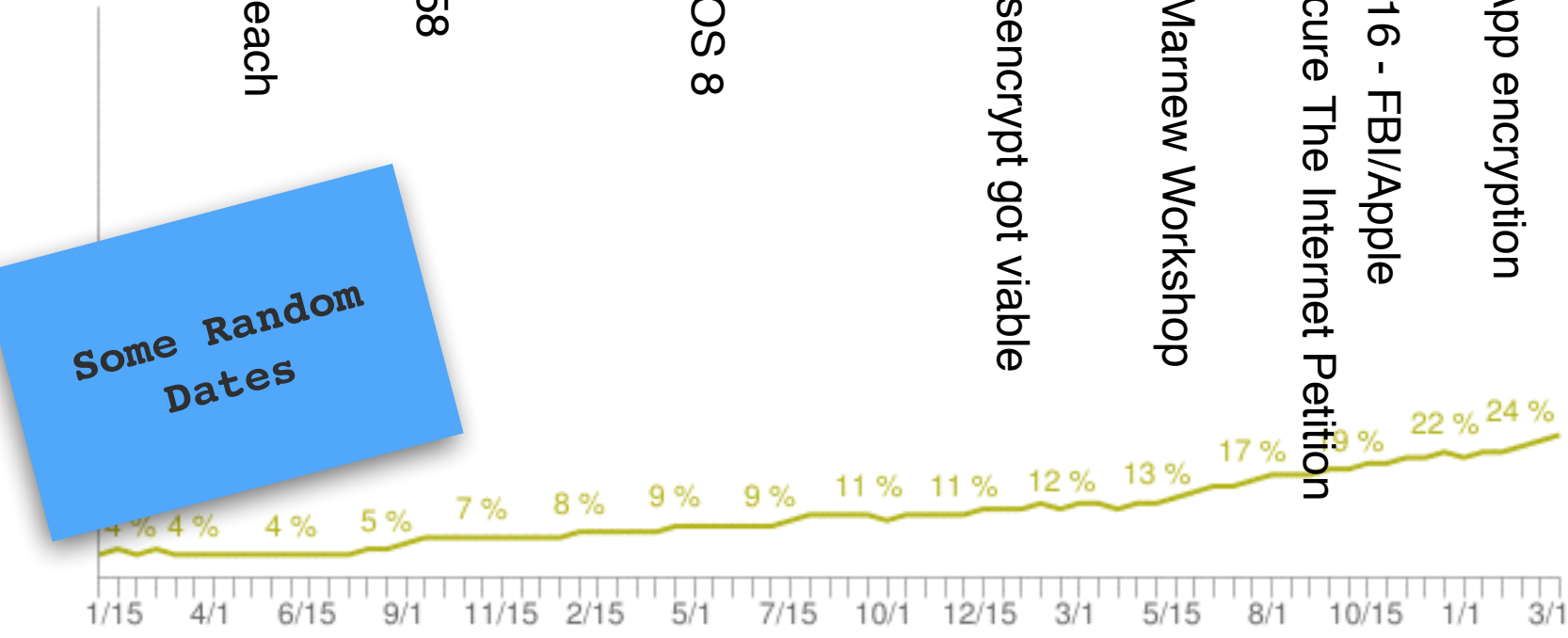
September 2015 - Marnew Workshop

February 2016 - Secure The Internet Petition

February-March 2016 - FBI/Apple

April 2016 - WhatsApp encryption

Some Random Dates



http://httparchive.org/trends.php?s=Top1000&minlabel=Jan+1+2013&maxlabel=Mar+15+2016#perHttps

And this week

US pushes Apple for access to iPhones in criminal cases

8 April 2016 | Technology

The Department of Justice would like access to an iPhone that is part of a drugs case in New York

Getty Images

The US Department of Justice has said it will pursue its request for Apple to help unlock an iPhone that is part of a drugs case in New York.

A letter filed to a local court said the government "continues to require Apple's assistance".

Source: http://www.bbc.com/news/technology-35996566

And this week

#FeinsteinBurr

SEC. 3. REQUIREMENT FOR PROVIDING DATA IN AN INTELLIGIBLE FORMAT UPON RECEIPT OF A COURT ORDER.

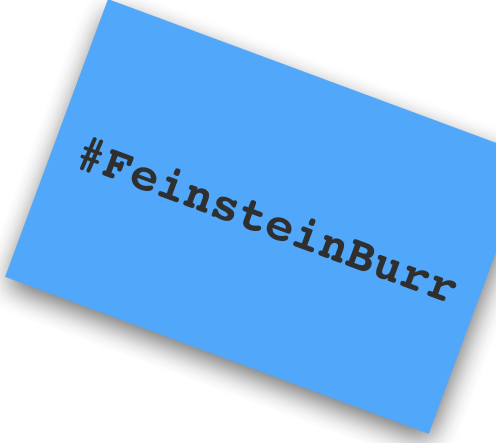
(a) REQUIREMENT.—

(1) IN GENERAL.—Notwithstanding any other provision of law and except as provided in paragraph (2), a covered entity that receives a court order from a government for information or data shall—

(A) provide such information or data to such government in an intelligible format; or

(B) provide such technical assistance as is necessary to obtain such information or data in an intelligible format or to achieve the purpose of the court order.

Internet Society


#FeinsteinBurr

Internet Society Resources on encryption

http://www.internetsociety.org/encryption

Policy Brief on Encryption is being finalized after review period ended April 1

Tech Activities

Internet Architecture Board
Internet-Draft
Intended status: Informational
Expires: August 24, 2016

R. Housley
Vigil Security
K. O'Donoghue
Internet Society
February 21, 2016

Problems with the Public Key Infrastructure (PKI) for the World Wide Web
draft-iab-web-pki-problems-01.txt

Abstract

This document describes some of the challenges facing the current Public Key Infrastructure (PKI) used for the World Wide Web (Web PKI) and considers promising improvements to address these challenges. Technical, process, and policy improvements to the WebPKI are considered. In addition, some technical considerations beyond WebPKI itself are considered. Hopefully the content of this document will help drive the Internet community toward wide spread adoption of so

the highlighted recommendations.

itted in full conformance with the

Networks & Trust

Introduction to PKIs & CAs

1 APRIL 2016

Directed at deployment and improving Internet scale trust infrastructure

From Encryption to System Security

ISOC's General Principles

Encryption should be the norm for Internet Traffic

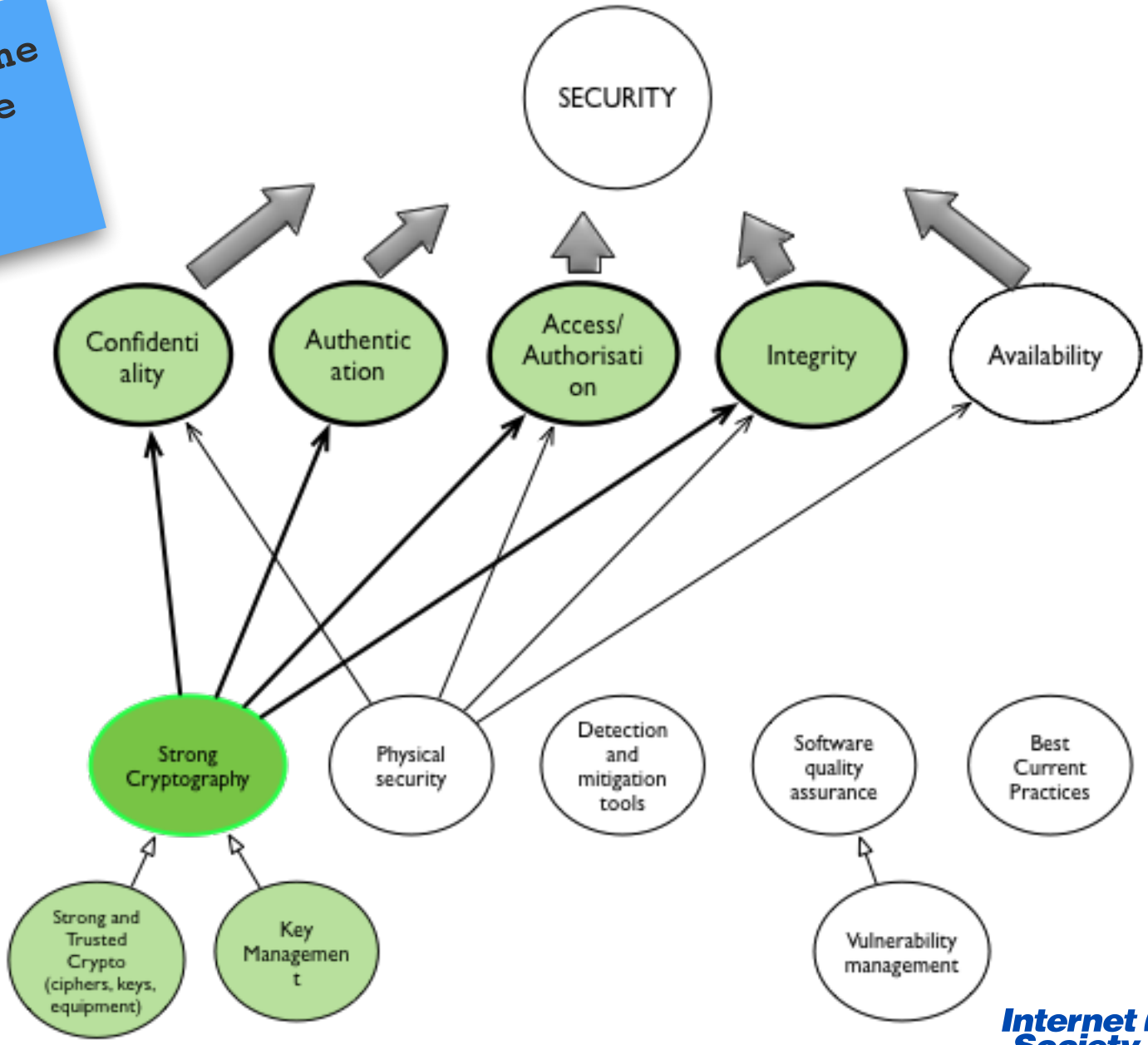
Weak Encryption is as bad as no encryption

There is a strong technical consensus in the tech community that Cryptographic backdoors are no-go territory.

Nuances

Encryption may impact operations and law enforcement activities

Encryption one tool in the security toolbox



The FBI/Apple Case was not about Encryption

Can a company be compelled to weaken its products security?

A few thoughts…

System Security Principles

It is my* belief that:

***Industry* is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system's security**

They should be empowered to create the best possible security solutions for their products and services

Industry should, under parameters of rule of law, cooperate with law enforcement, whilst not sacrificing the principles above.

Governments should create the best circumstances for improving System Security.

* This is not (yet) ISOC's position

System Security Principles

It is my* belief that:

…place to assess risks, cost and benefits, and …al solutions hence they have a primary …or the …m's security

They should be empow… …he best possible security solutions for their p… …vices

Industry should, under parameters … rule of law … …operate with law enforcement, whilst not sacrifi… …les above.

Governments should create the best … …or improving System Security.

Not just a Law-Enforcement issue

A general Cyber Security issue

Broadly applicable

Including IOT

* This is not (yet) ISOC's position

Some Questions and observations

Governments should create the best circumstances for improving System Security.

That means: Responsible disclosure, bug bounties, procure for security, setting high security expectations, etc, etc.

That does not mean: prevent the general public from '*tinkering*', '*hacking*', and security research

But how does that relate to the use of exploit kits by law enforcement?

What prevents proliferation of the tools to enable strong system security such as encryption?

Some Questions and observations

Industry is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system's security

For sure they are not the only actors: system security is the responsibility of many parties, including governments (public safety) and users themselves

Some Questions and observations

Industry should, under parameters of rule of law, cooperate with law enforcement, whilst not sacrificing the principles above.

What are the needs for industry to work with law enforcements and vice-versa

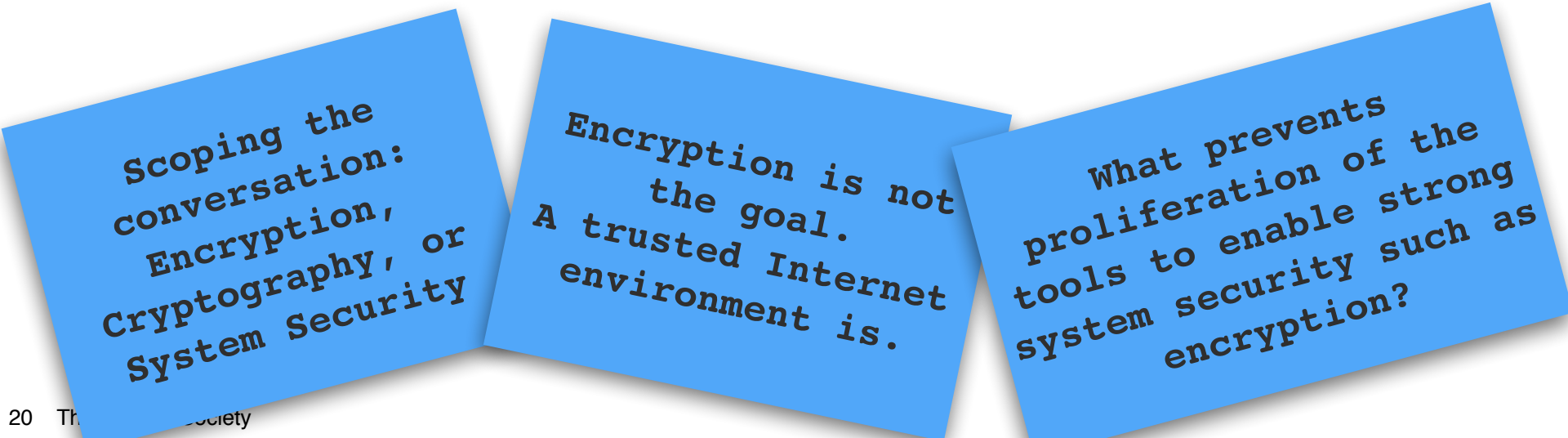
Additional nuance is needed. There is a difference between cooperation/assistance and becoming a tool of the government

How about the procurement and use of (existing) exploits by law enforcement?

Some Questions and observations

Are the issues different for data in motion (traffic on the Internet) and data in rest (on some device)?

With encryption the norm for communication the only way to get to data is at the endpoints, which makes system security relevant to focus on.



Some Questions and observations

Industry is best place to assess risks, cost and benefits, and viable technical solutions hence they have a primary responsibility for their system's security

Does that work in global context: what are the specific issues in cross-border cooperation?

TXkIdbsHSVWaIdwZvYImcBo4taN0hpp9zmQd3EgyG1+60vLtPXMgMhQwOQ9OOECUeo3+HdqnOvqs77rzPOMPcHNoZAQVPgrImXTYfGhl7gsWfzOxF
Y954CC5QeHoG+11oUMjLu5uRu358TaGlYbH17CG7mBk+fedEhmRc7+VJL8co3A7W2xyqzN
+AADV09FxewRp5i8vSsOibxJCwFzOknQmHXcXG80KtNsKaMACRWZPaWTB84b1HI
+9D23XhYeCmzhzaHqRjivQuBpC7KS5hf1odjjmOk0f6rEIkAgE4QQ4H2wKwe1sp6plESKYmUdAx9ik2nlqbLxDneZJG4xNfSR0D0X9gX8/
aY8TTRWf7oH8GmfOebcFGtLbXvkRv2YjumPvNRmScPfZml3ouQahX1j+0IqypHq7J9NA5hppQr0DQ1FW0ClPQIm92TdO/
bJOIqjRlgdYYkJBXJWQZtnLZpqi/sDuAGag5kbLPVAoGT3rDLQ0uQpopR/
zJKVAcnfXFFWOfQLTPz4t03xHK2rm4kwcgVLl8quzRn5ZRZXU26TGpM7iCNkrihhL5R1hPjIXwcRSaowVd8lXuM/
QgF68h1oTla8Ybl00q1Iis3qp1ZhuP33LgElYKbhak9x20ZC/t+P7Vf9rh9K4o/3RNl9Tv60Cp885i40IynFwWEbaDzQTVoV3rGHwz5mjQHSy/

What are your thoughts?

iiigPChPZTg94yck18astDFdSvguUT0536jBaZfuL0ZWaadw1Edoz6trK9YK13yysPcBXIRUQXRpKkI/Zs/
MHtVKXP769AZTHmicrV9pvnXAysVBcuLLwQLpez9HcQTBSTyFW46WwAcYvVEvE8F0hAp+ju0g6sVUsz3SnHGmP6/
TXkIdbsHSVWaIdwZvYImcBo4taN0hpp9zmQd3EgyG1+60vLtPXMfIuOXlljv1/5zni5j/zc+bZLbL4x+5ZBCfi3hu7vyI
+IhQSuMqLEYFWGHIHIcxnOZj6AXj3b6t9xkqd37Q37WdscBR8hfoQcjwxY2nzcW7DWYtCpD0CgrLwQzR574g040te/
kz5veOrNXjQ8AUaVRh2zFJC2/+vcjcnIvNtsb1lgI764EgRcNcbvX17s0+insjOd3wiQLnNUkArLW0Elji6mFuguQAByXdIFCDVf6qDQPaQIf6v0JGjAMzWwCu6D7kXj
lRK3DZdzOEZK+fD4zZHTADwusNFPddCrp3QUlkp0R5/Wl+wDnZef53Fh+eQkdgjpEVvl1fCKYa9kZMSw3LaMjcl/L5c7c5RZgD4q6vXFpDGuxoEJmRmVDnPiW
+gx0m7lxuWgnNbpTwSqrGEiQrfnDsc1U5gTk8TCmJqGkxWcTDEJdw0jHplAFlJub84cd7nDJObxVPWQXz2CI/ndTiLCRSH2Iople7YWJxO3kF3L
+YrPtqXyBki8cBWQUg7rJQj3zr7myFXTHkGkiOB5x47q53rHdqyxEwTmdNXA3sVb+JQFCAupavLu
+mCnzlNoSqE4DLz56VIjrbanvlZwityr9oRWq7AsNIvPVXUAx6MfgjL7aviZ6oJpKa7BiTaNgeuR/LRUIJFf/
mzdNz4EcdmLOUpWznR2pI33yJyF2hw9csDtmVcv8d9XFSq1uFPnqaxjEaRae3YwIcGuVnOSk21M3hWNMWuZdoVwunxWbOHuhK5u8qSdIjZHzwWSdo/jkRRyGsn/
32McahXQYE7KBeTD3aoHCufHVSQjunhxOLSd96D2lzFNlSQSjXhlCYmTqqOTSQYLvkIJ/FPTRvYibriptCmOepisMZV1udIBNXD+zligYJ
+JvhdCCIsDyGOEhKz8Yt70QbG/lg89jhC6nAxEgaaFhpRIc6nNeFU3lE9nqe8N/rng4xOwaS5h6d4X5RZwmEnE/
gMhQwOQ9OOECUeo3+HdqnOvqs77rzPOMPcHNoZAQVPgrImXTYfGhl7gsWfzOxFY954CC5QeHoG+11oUMjLu5uRu358TaGlYbH17CG7mBk
+fedEhmRc7+VJL8co3A7W2xyqzN+AADV09FxewRp5i8vSsOibxJCwFzOknQmHXcXG80KtNsKaMACRWZPaWTB84b1HI
+9D23XhYeCmzhzaHqRjivQuBpC7KS5hf1odjjmOk0f6rEIkAgE4QQ4H2wKwe1sp6plESKYmUdAx9ik2nlqbLxDneZJG4xNfSR0D0X9gX8/
aY8TTRWf7oH8GmfOebcFGtLbXvkRv2YjumPvNRmScPfZml3ouQahX1j+0IqypHq7J9NA5hppQr0DQ1FW0ClPQIm92TdO/bJOIqjRlgdYYkJBXJWQZtnLZpqi/
sDuAGag5kbLPVAoGT3rDLQ0uQpopR/zJKVAcnfXFFWOfQLTPz4t03xHK2rm4kwcgVLl8quzRn5ZRZXU26TGpM7iCNkrihhL5R1hPjIXwcRSaowVd8lXuM/
QgF68h1oTla8Ybl00q1Iis3qp1ZhuP33LgElYKbhak9x20ZC/t+P7Vf9rh9K4o/3RNl9Tv60Cp885i40IynFwWEbaDzQTVoV3rGHwz5mjQHSy/DL5jJvt/
G4CotmWgHfUsMiLlhYvLZH8BLBdMJ3lmAMGzK0xusumcguQRckHvyEyUi+WODyByrq5LmED/8tDiPIqsHo7I4+PgmxAKwG4T5TmHCrUgFFt48zX/a0fYIARbHhw3zT/
H6RM2Thvu8THdA9oAB5YfZy6wwMtkdW0uRDDkUyiAHPIvg5YQPpC5b1XEipF0oxksNPIa2jTNLDCwnwlU6DWYEq7vIexn9OqHVlYhp1mCsKTZdPw1d8gGOwthYdRxmAI
Pe/wc9CXVmj4e8SELz9jrORCHXb82uF+JMik4c4z428bBQ66SPCP8K2EONXOH17CK11NFv1BHTR5CCI0GVphf3GC0krUEUJJWT
+qz4BqUdBCllpIAQCsUt5m3leVTCZDt7gQmCR6UbrBFtHgJ/8T8Ysh/zS2+x7iCUTypR4t5NXhoMSCx44BB3q91+yVKQvzu3iIrYOij9WNdXkzn1n9KXwv
+46Ul4ZHH3X3Q0QqljXO6r+Doy1Nn+1/CLEAIXdZJo/J1QMpcaIUseqtCnsiwodZMmCfRLBqadgqL+sbsTqhIZX1mcYk1+n
+tBCN5p0ezvIEEIoBTPYHGtBdAvzVmVNrd4g5lzHKJExLw2Akn4k6yhQZPIkZwXtd6pUgfoIuiJvpjhPemeEvKp7YFlzkH1TnRvV87zsDHSigrHIjpiLLGXEYnbmPh5a
ecc386zm8CODp4k+11gWI2Q3tsrLhx+leG8GjmIfF4OW7fGJDF1IR8yI7FLkv6aPR5SH5PntuNr6/nqVlq/ZfxtOU+gpRzMhJlb0Mp+yzYpc3ysGzMTjhr5+0mc8g4/
EkyLg4FzHrSmow+3REMCM+XYrvsNy54A=

Internet Society

Olaf M. Kolkman

Chief Internet Technology Officer
Kolkman@isoc.org
twitter: @kolkman

Internet Society™