Crypto as Global Business

2014 for

Mika Lauhde
Vice President, Government Relations and Business Development
SSH Communications Security

Working with Critical Government Infrastructures

- **Member of ENISA (European Network and Information Security Agency) PSG (2009 -)) (Part of the European Cyber Security Strategy plan 2013)**
- **Management member of Leuven University European Crypto Task Force (2014 -)**
- **EU ENISA – Europol working group (2014 -)**
- **Management member of European Cyber Security Research Center, (2011 -)**
- **Member of Finnish Government Cyber Security working group (2013 -)**
- **Founding Member and Board Member of TDL (Trust in Digital Life) (2010 - 2013) (Part of the European Cyber Security Strategy plan 2013)**
- **Member of EU government security advisory board RISEPTIS, reporting to Commissioner Reding), (2007-2009)**
- **Member of Finnish government ICT security advisory board (2007 – 2010)**
- **Member of UK government critical infrastructure protection group CPNI (2005 – 2009)**

All views and opinions in this presentation are the author's private views and opinions

Any resemblance with company or institution views and opinions is purely coincidental

History of encryption

Beginning of SSH Communication Security

Tatu Ylönen

Tatu Ylönen,
Chief Innovation Officer

While working as a researcher at Helsinki University of Technology, Tatu Ylönen began working on a solution to combat a password-sniffing attack that targeted the university's networks. What resulted was the development of the Secure Shell (SSH), a security technology that would quickly replace vulnerable rlogin, TELNET, and rsh protocols as the gold-standard for data-in-transit security.

Tatu has been a key driver in the emergence of security technology including SSH & SFTP protocols and co-author of globally recognized IETF standards. He has been with SSH Communications Security since its inception in 1995 holding various roles including CEO and CTO and as a Board Member.

In October 2011, Tatu returned as the Chief Executive Officer of SSH Communications Security, bringing his exceptional experience as a security innovator to the company's product line. In October 2014, he changed to the role of Chief Innovation Officer in order to be able to focus more on the technology-side of the business. In this role, he is responsible for selected new product concepts, the company's intellectual property development, and various other strategic initiatives.

Tatu holds a Master of Science degree from Aalto University, Finland.

Antti Huima,
CTO & Vice President, Engineering

Antti heads the company's global R&D and directs the company's technology strategy. He has nearly twenty years of experience in the software industry with extensive experience in information security, cryptography, software quality assurance and theoretical computer science. Prior to joining the company, Antti served as CEO at Conformiq, a Silicon Valley based software test design automation company.

Before joining Confmiq, Antti was Research Manager at SSH Communications Security leading contribution to the software architecture. Antti has lectured cryptography, computer security, and theory of testing on university level and has served several academic program committees.

Antti has a Master of Science degree from Aalto University, Finland.

We Invented the SSH Protocol

SSH Communications Security

Quick Facts

Who we are

- Inventors of the SSH protocol
- NASDAQ OMX Helsinki (SSH1V)
- In business since 1995

Technology Leadership

- Leading author of 5 RFCs
- Influence on 98 RFCs
- Authors of IETF Best Current Practices for Secure Shell identity management

Customers

- 3000+ customers
- 7 out of top 10 of Fortune 500
- 40% of Fortune 500
- More than half of top 10 US banks

A Few of Our Customers

Energy

Governments

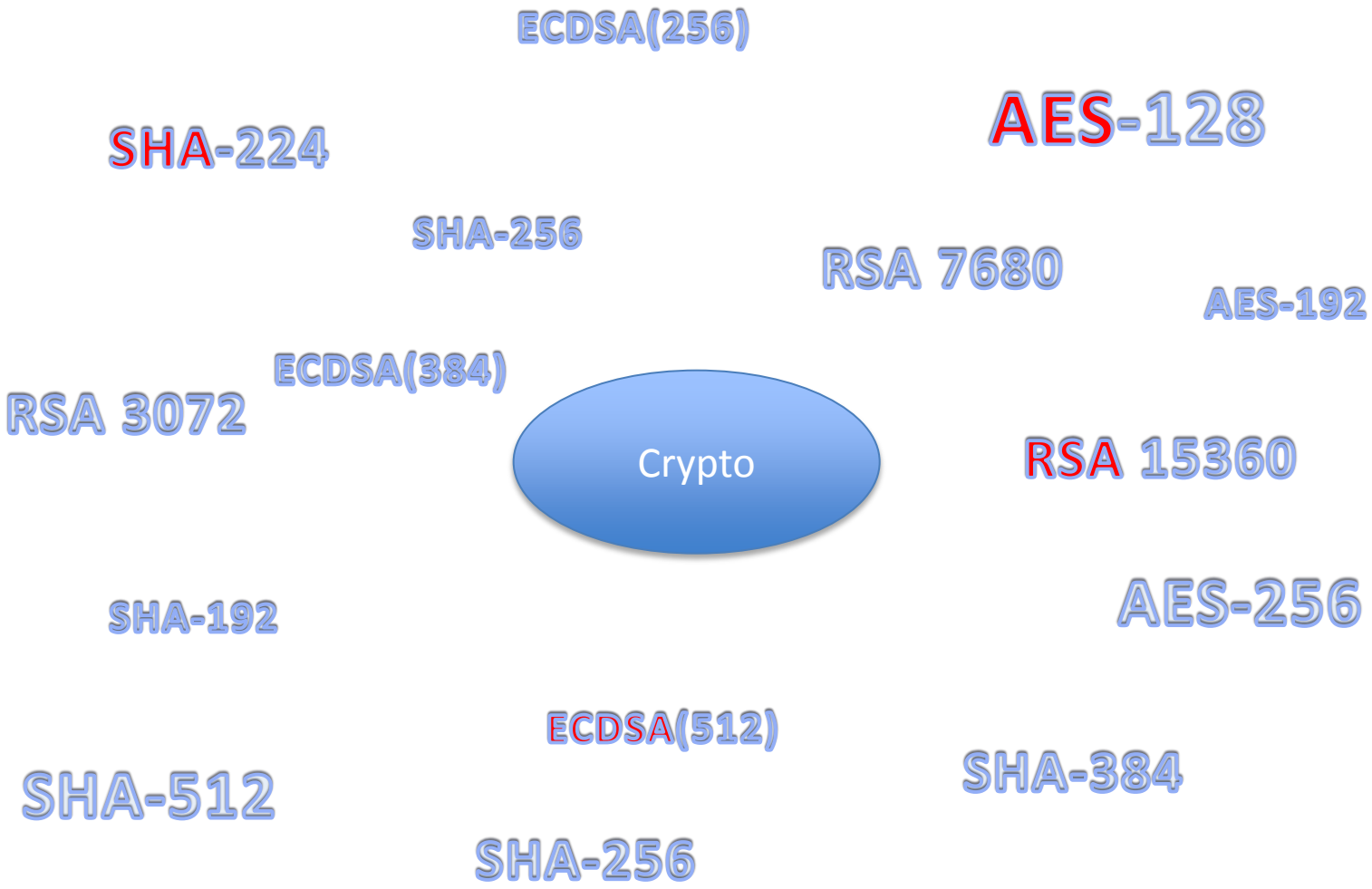
Banks

Retailers

Health care

Crypto

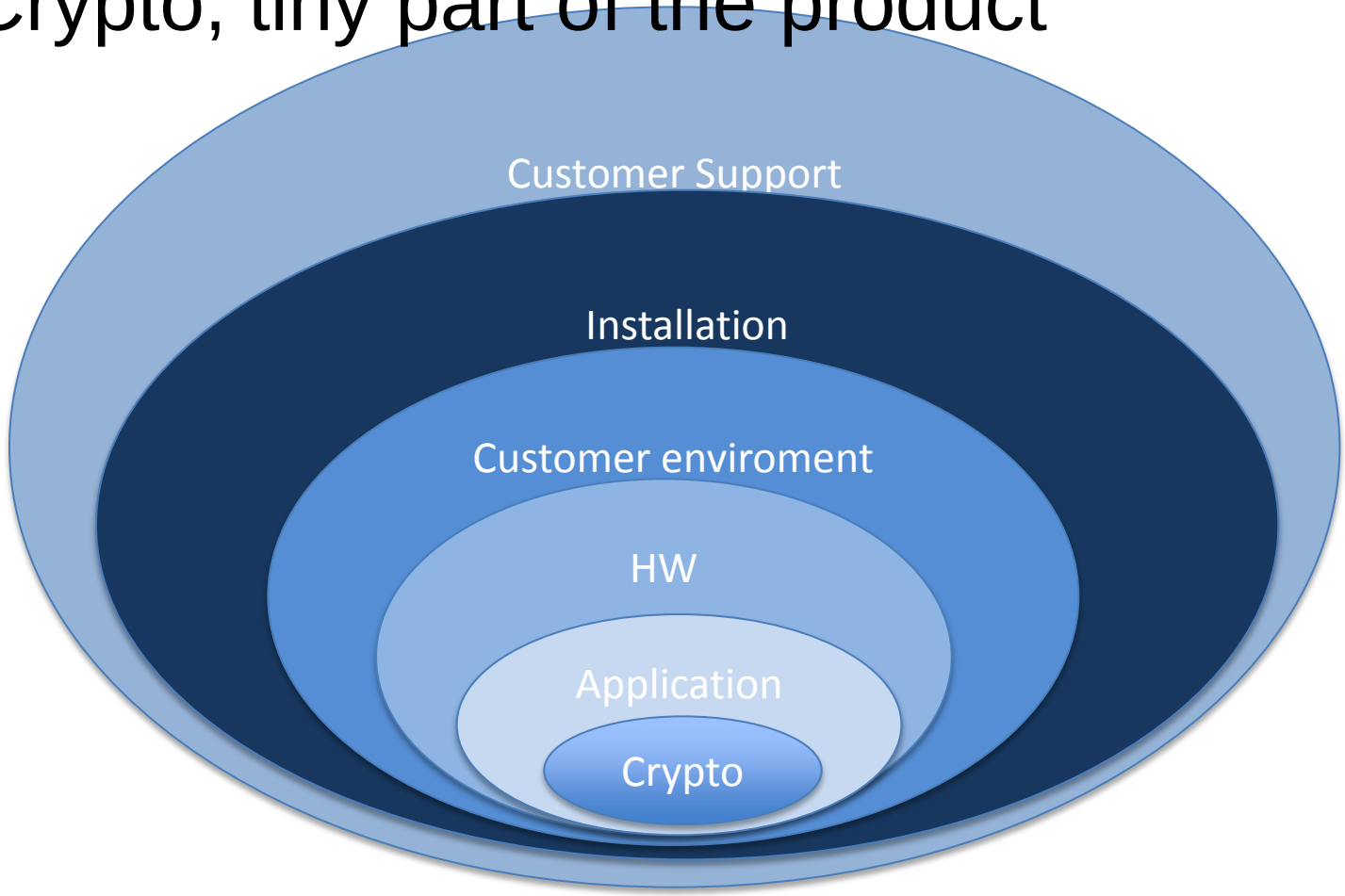
Crypto



In US you are NOT allowed to use these crypto's to protect material classified secret

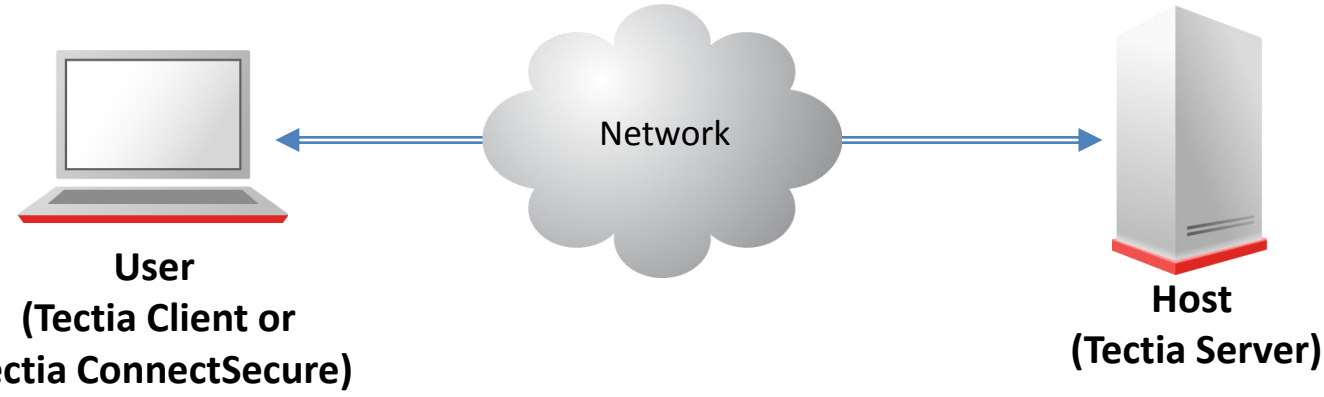
Crypto

- Crypto, tiny part of the product



Secure Shell: The essentials

- An application that encrypts the TCP/IP traffic between two end points (client/server).



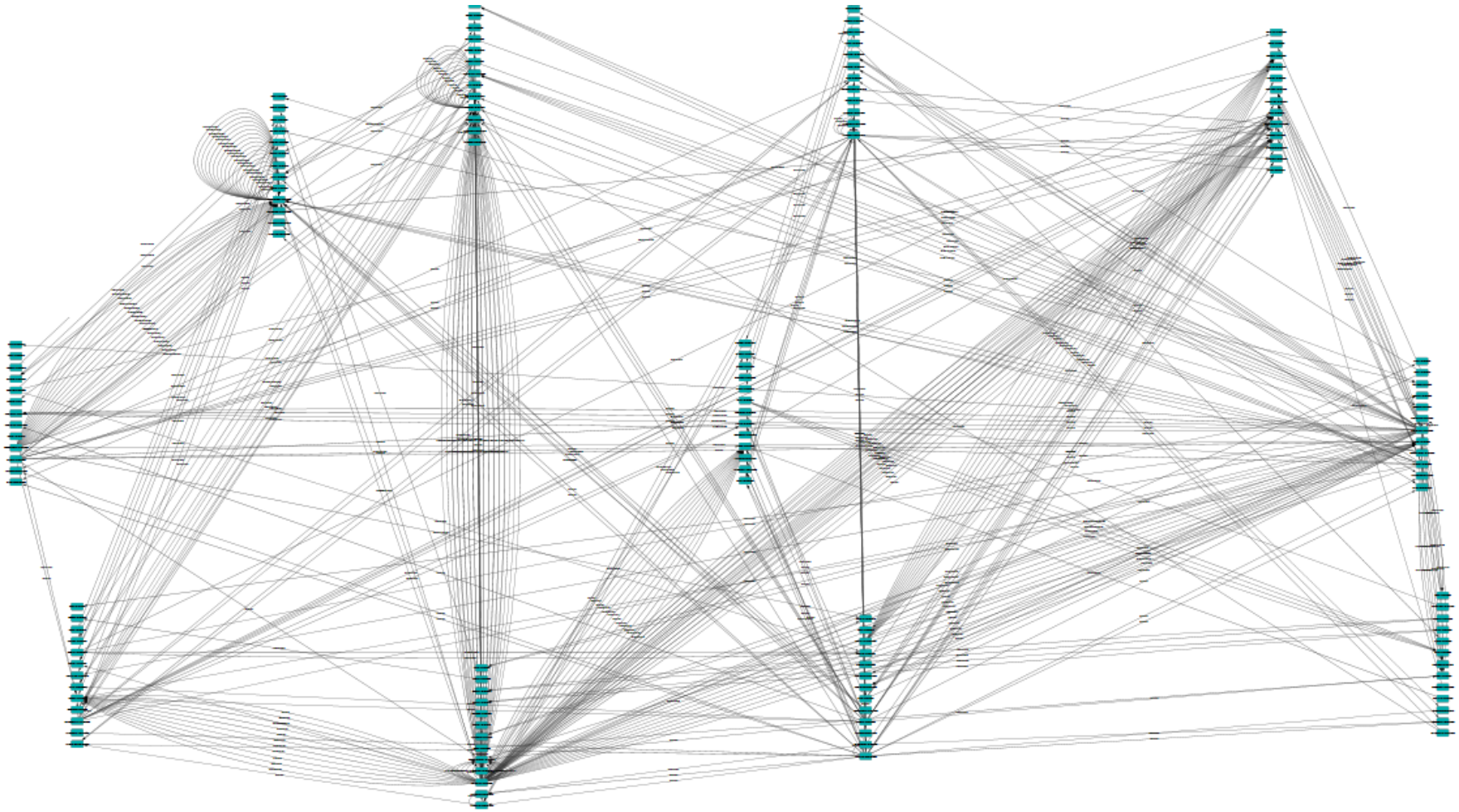
- Ensures that the information is confidential, unmodified and that the sender and receiver are who they claim to be.

Tectia SSH

Transaction Security

- Secure Remote Administration – Replacement of Telnet, Rlogin
  - Provides a secure alternative for the insecure commands
- Secure File Tr…
- …Application Connectivity, i.e. TCP tunneling/forwarding
  - Enables securing any TCP based traffic
  - Tectia ConnectSecure provides transparent and automated TCP tunneling

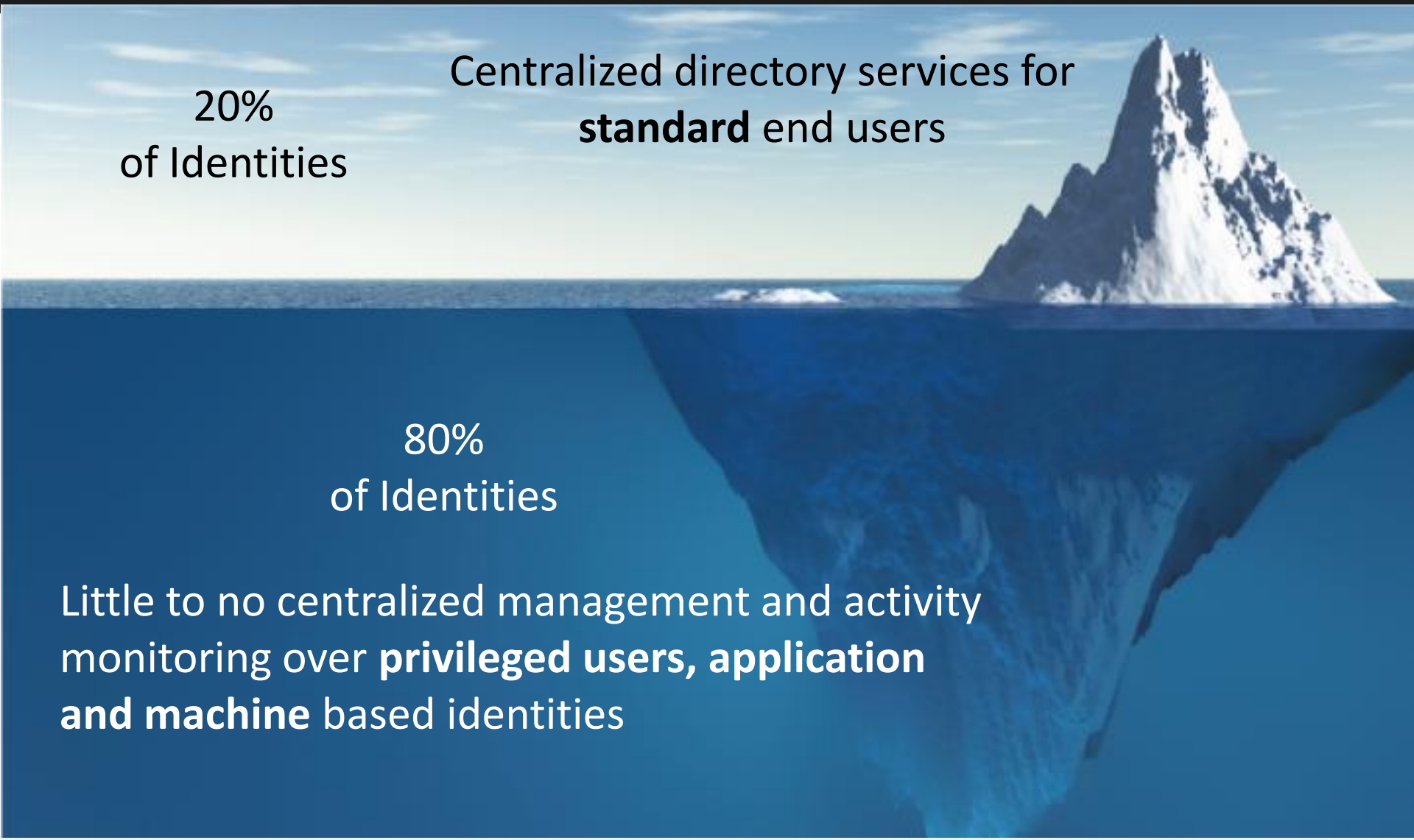
Real life…



Reality with encrypted tunnels

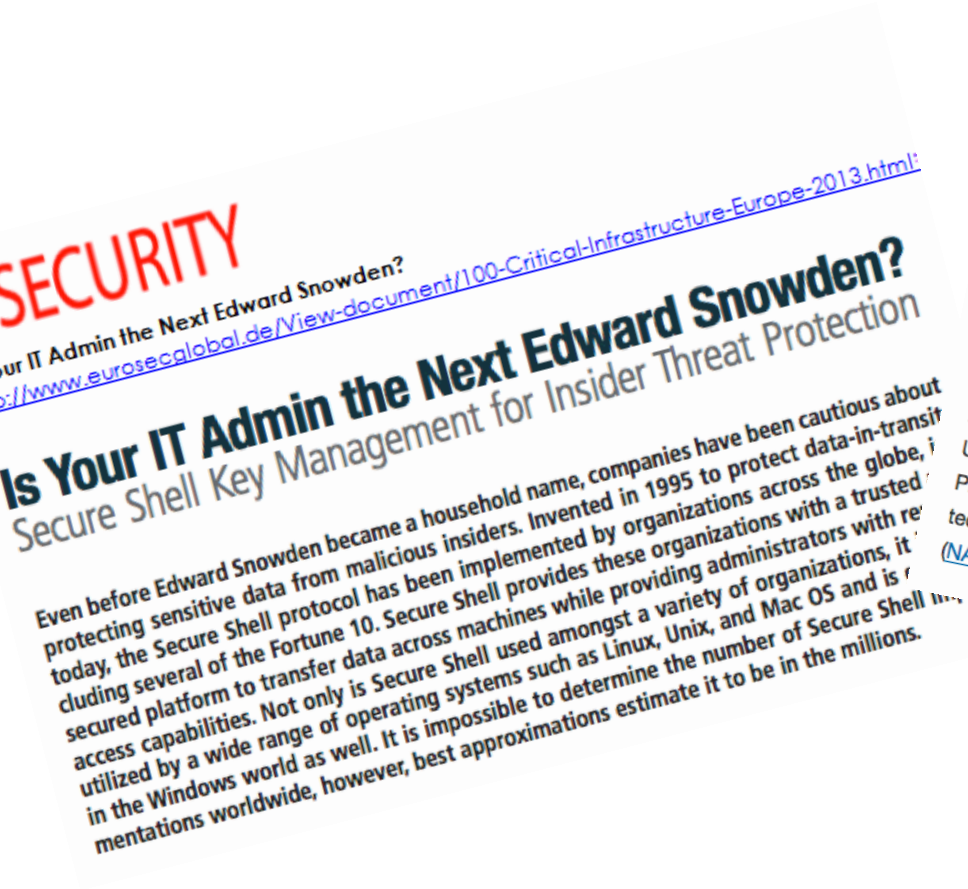
- From secured tunneling to unsecured maintenance
  - Monitoring of internal and external users

The Identity Governance Gap



SSH from east and west

- Same issue, different approach


SECURITY

ur IT Admin the Next Edward Snowden?

://www.eurosecglobal.de/View-document/100-Critical-Infrastructure-Europe-2013.html

Is Your IT Admin the Next Edward Snowden?

Secure Shell Key Management for Insider Threat Protection

Even before Edward Snowden became a household name, companies have been cautious about protecting sensitive data from malicious insiders. Invented in 1995 to protect data-in-transit today, the Secure Shell protocol has been implemented by organizations across the globe, cluding several of the Fortune 10. Secure Shell provides these organizations with a trusted secured platform to transfer data across machines while providing administrators with re access capabilities. Not only is Secure Shell used amongst a variety of organizations, it utilized by a wide range of operating systems such as Linux, Unix, and Mac OS and is in the Windows world as well. It is impossible to determine the number of Secure Shell mentations worldwide, however, best approximations estimate it to be in the millions.


WALL ST. CheatSheet SAVE TIME. MAKE MONEY.

Lost the Key to Your Data? The NSA May Have Picked It Up

http://wallstcheatsheet.com/stocks/lost-the-key-to-your-data-the-nsa-may-have-picked-it-up.html/?a=viewall

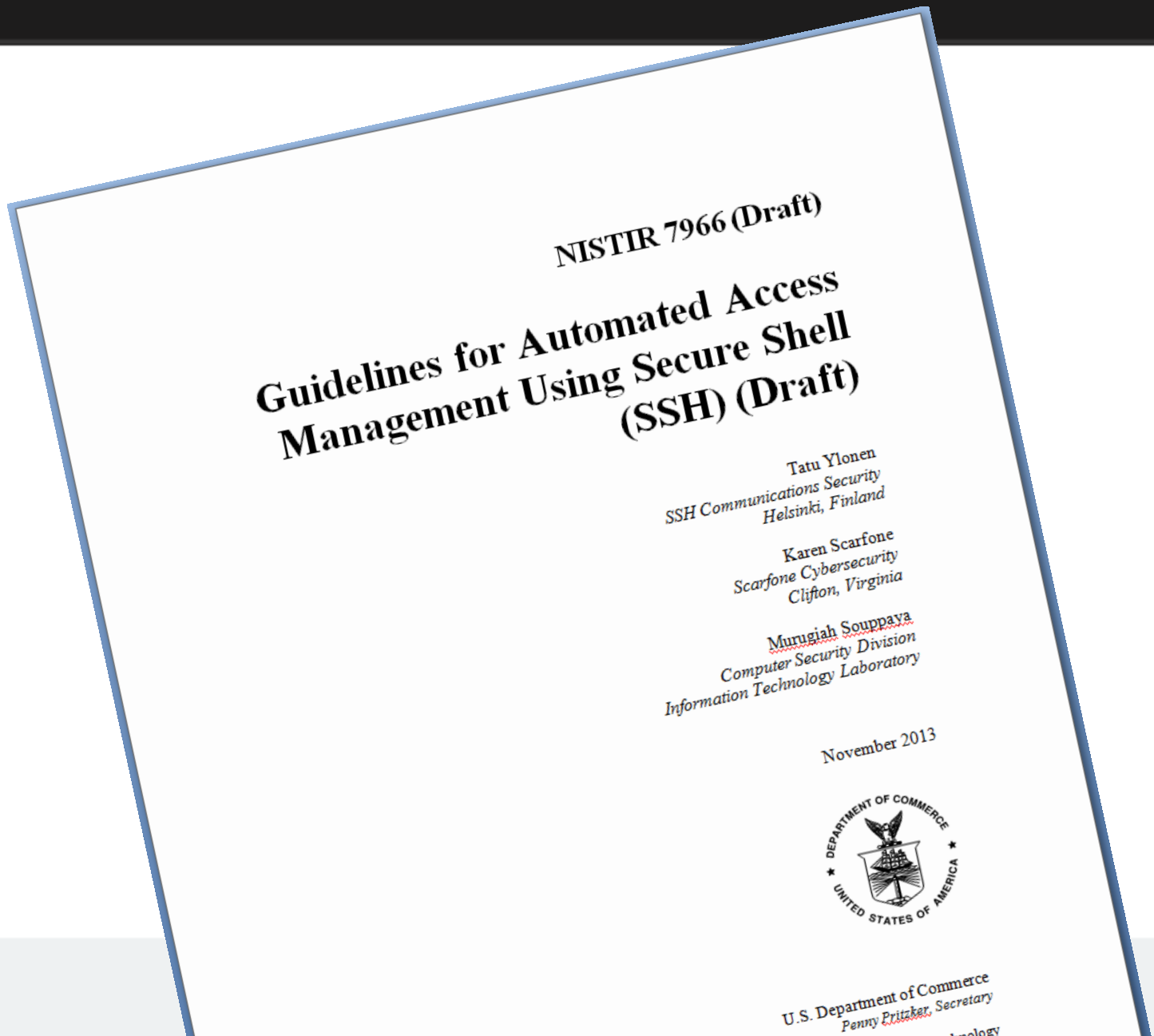
Lost the Key to Your Data? The NSA May Have Picked It Up

DAN RITTER | MORE ARTICLES

SEPTEMBER 28, 2013

In May, Edward Snowden — once a contractor for the U.S. National Security Agency — leaked information related to top-secret mass surveillance programs conducted by the United States and the United Kingdom to the U.K. newspaper *The Guardian*. The report states that through a program called PRISM, the NSA has been able to obtain direct access to the systems of major U.S. Internet and technology companies such as **Apple** (NASDAQ:AAPL), **Google** (NASDAQ:GOOG), **Yahoo** (NASDAQ:YHOO), **Microsoft** (NASDAQ:MSFT), and others.

Contribution for standards...



NISTIR 7966 (Draft)

Guidelines for Automated Access Management Using Secure Shell (SSH) (Draft)

Tatu Ylonen
SSH Communications Security
Helsinki, Finland

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

November 2013

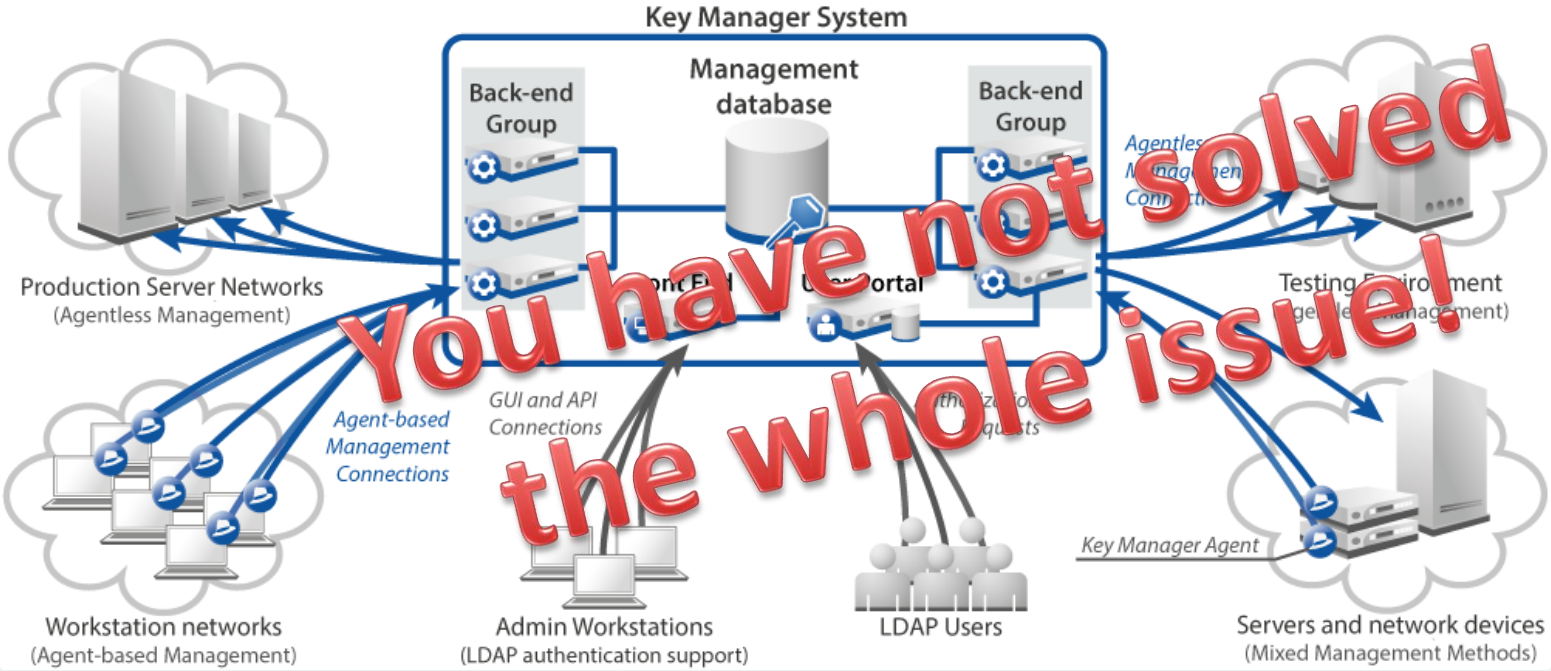
U.S. Department of Commerce
Penny Pritzker, Secretary

Universal SSH Key Manager

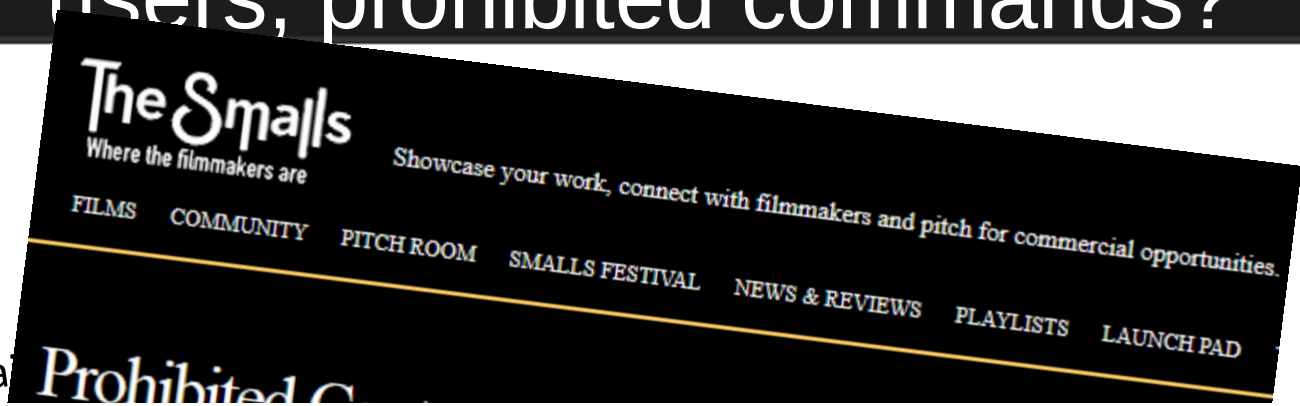
Management & Governance

Discover → Monitor → Lockdown → Remediate → Manage

- Hosts, Users, SSH Keys and Trust-Relationships
- Logins and Key Usage
- Unauthorized Operations
- Relocate Keys and Lock Down Servers
- Remove Obsolete and Policy Violating Keys
- Automate and Integrate Life Cycle Management of Your SSH



Prohibited content, prohibited users, prohibited commands?



Adult content

Information Security Stack Exchange is a question and answer site for Information security professionals. It's 100% free, no registration required.

Take the

PCI - prohibiting direct connections to the Cardholder Data Environment

2

1

In PCI 1.3.3 it states:

> Are direct connections prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?

A Cardholder Data Environment (CDE) encompasses any device or server that stores or transfers cardholder data. (PCI Glossary available here)

With our system, a user adds a credit card via the web, making each one of our front-facing servers a part of the CDE. In my view this is a paradox because any server the user has a direct connection to will always be considered a part of the CDE

asked 22 da
viewed 35 ti
active 22 da

Related

0 PCI-DSS fo POS on sa

3 Can we prin data under

Privacy Policy
Content Protection
Child protection

necrophilia).

To this end,
Player. You
boulevard
question,

Standard Bank Group's growth in promoting sound financial advice and to allow experience with us (Standard Bank Group). This section is not a forum to get answers relating to specific queries or issues or register complaints.

Prohibited content

We (Standard Bank Group) believes in freedom of speech and expression. H

users, the following content will not be permitted:

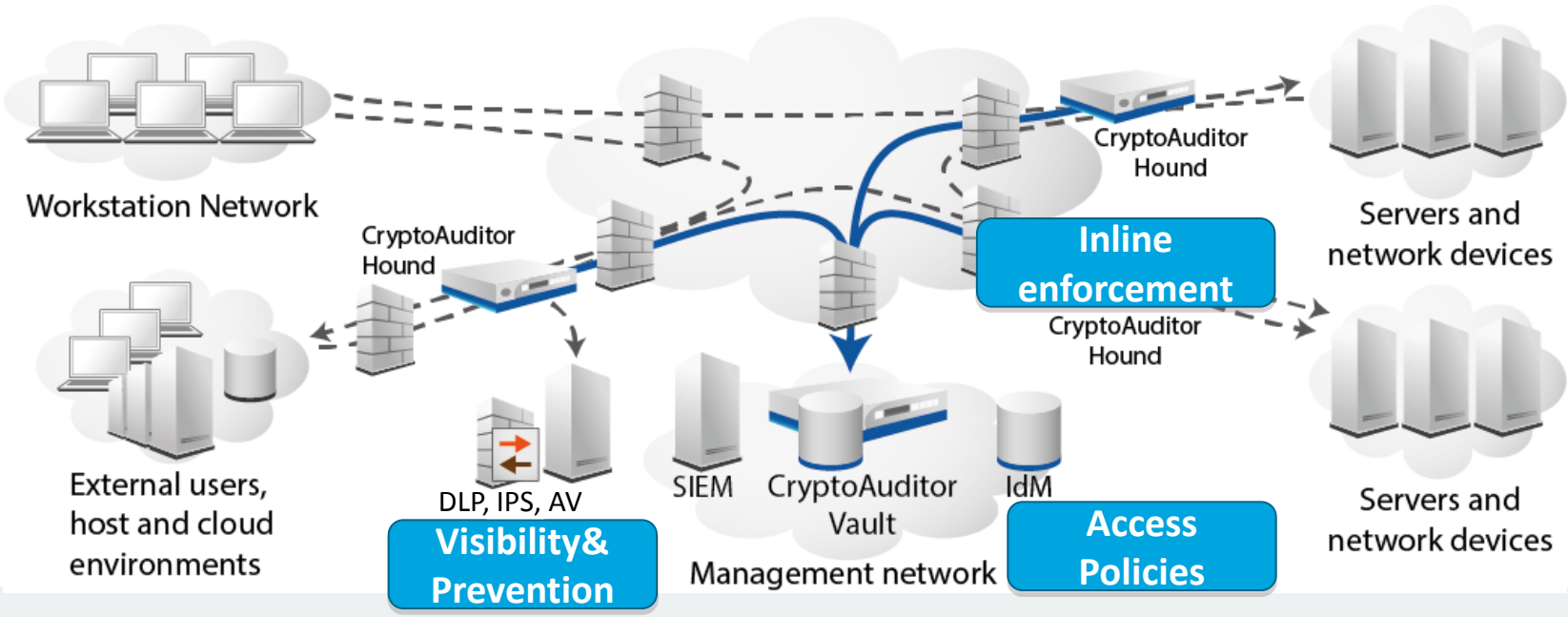
1. Content that is or may gene

pornograph

CryptoAuditor

Content Aware Access Management

- Deep Protocol Inspection (SSH/SFTP, RDP, sub-protocols)
- Full session visibility and recording
- Real time session indexing, alerts and enforcement
- Layered defense enablement (DLP, IPS, AV)
- Distributed, transparent deployment and operation



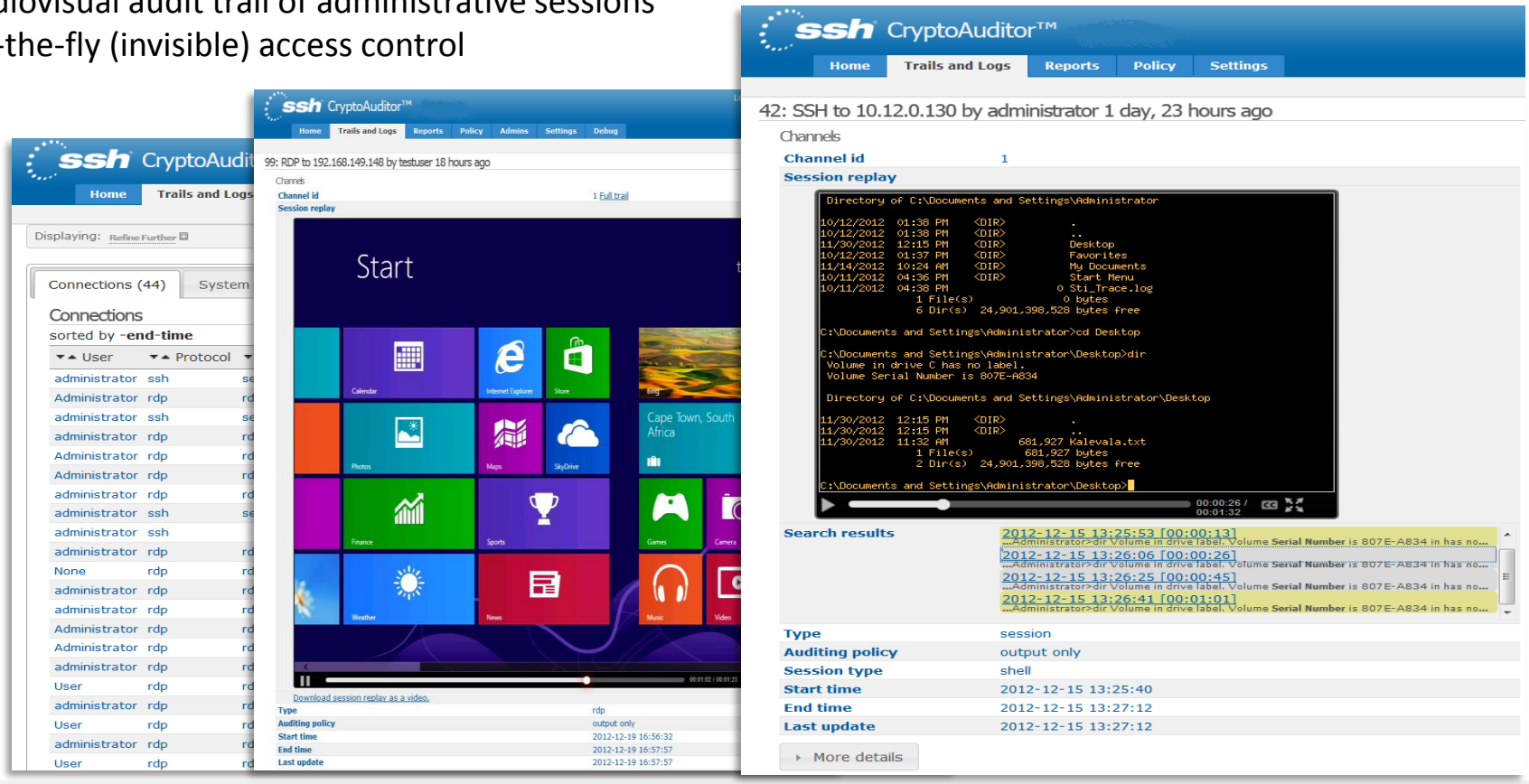
Solution to see trough encrypted tunnels

SSH CryptoAuditor - Privileged user access control and audit ”on-the-wire”:

→No sign-in portals

→No client or hosts agents to control access or gather audit trail

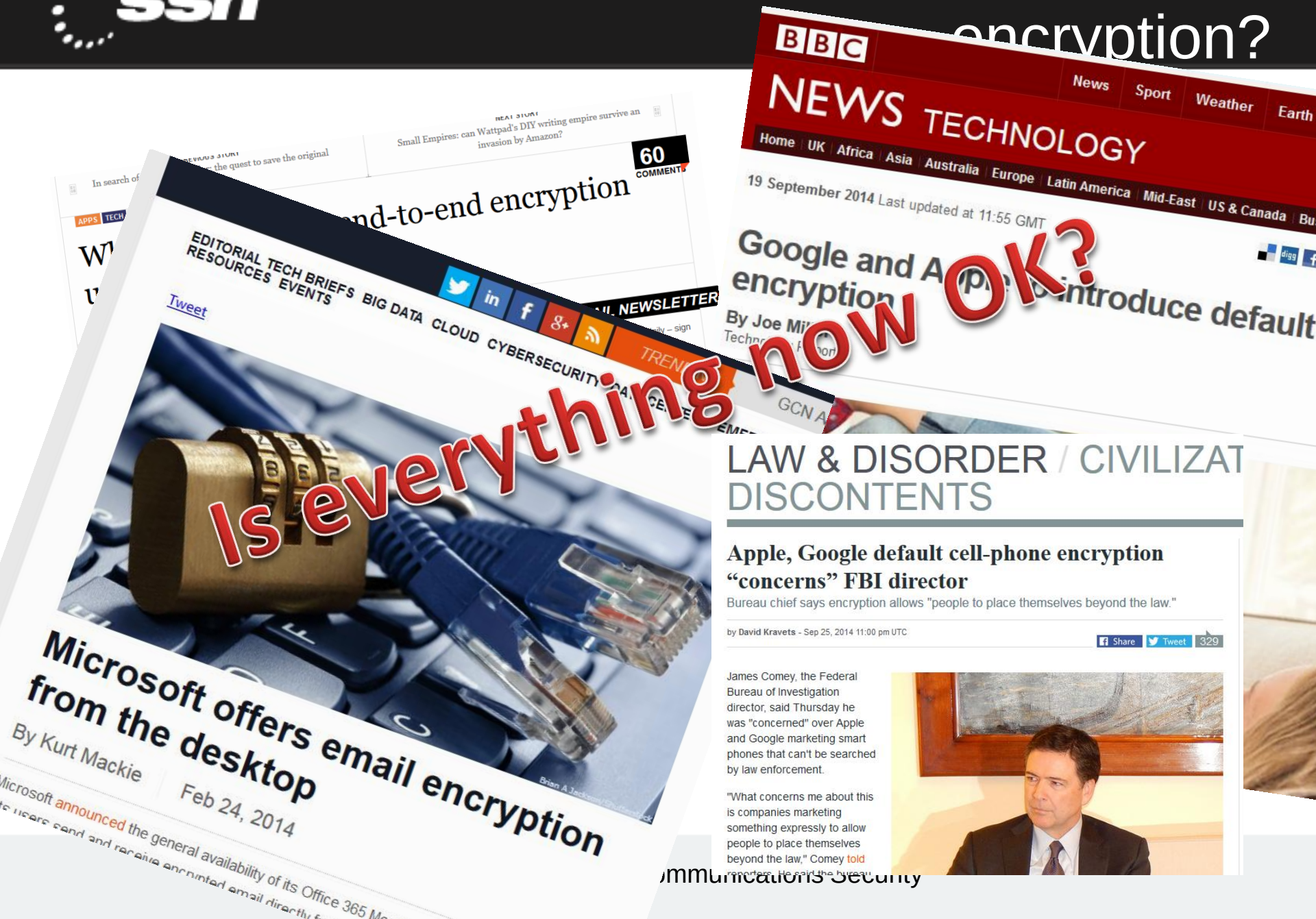
- Optical Character Recognition (OCR) to index and inspect session activities
- Audiovisual audit trail of administrative sessions
- On-the-fly (invisible) access control



What Snowden told you?

I have nothing to hide……

Now everybody are announcing encryption?



mmunications Security

NO, NOW WE REALLY HAVE ISSUE WITH ENCRYPTION IN EUROPE

Thank You

Questions: mika.lauhde@ssh.com

Mika Lauhde
Vice President, Government Relations and Business Development
SSH Communications Security
mika.lauhde@ssh.com