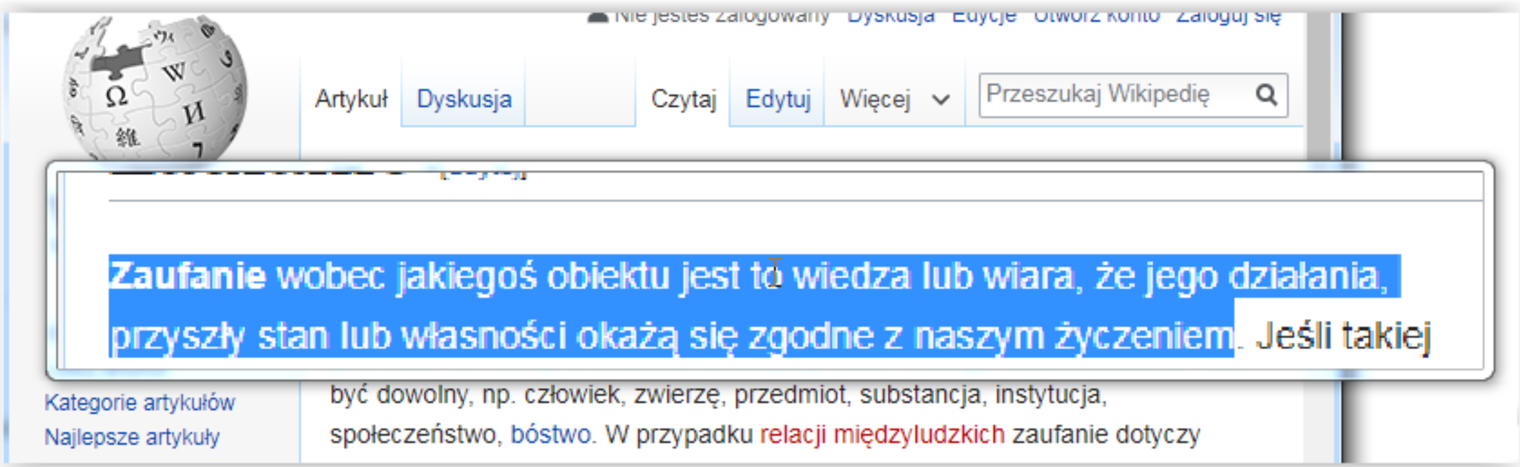
ROOT of TRUST

gemalto
security to be free

Piotr Wróbel
11’2018

ROOT of TRUST

zaufanie?!



Zaufanie wobec jakiegoś obiektu jest to wiedza lub wiara, że jego działania, przyszły stan lub własności okażą się zgodne z naszym życzeniem. Jeśli takiej

być dowolny, np. człowiek, zwierzę, przedmiot, substancja, instytucja, społeczeństwo, bóstwo. W przypadku relacji międzyludzkich zaufanie dotyczy

ROOT of TRUST

obiekty zaufania?!

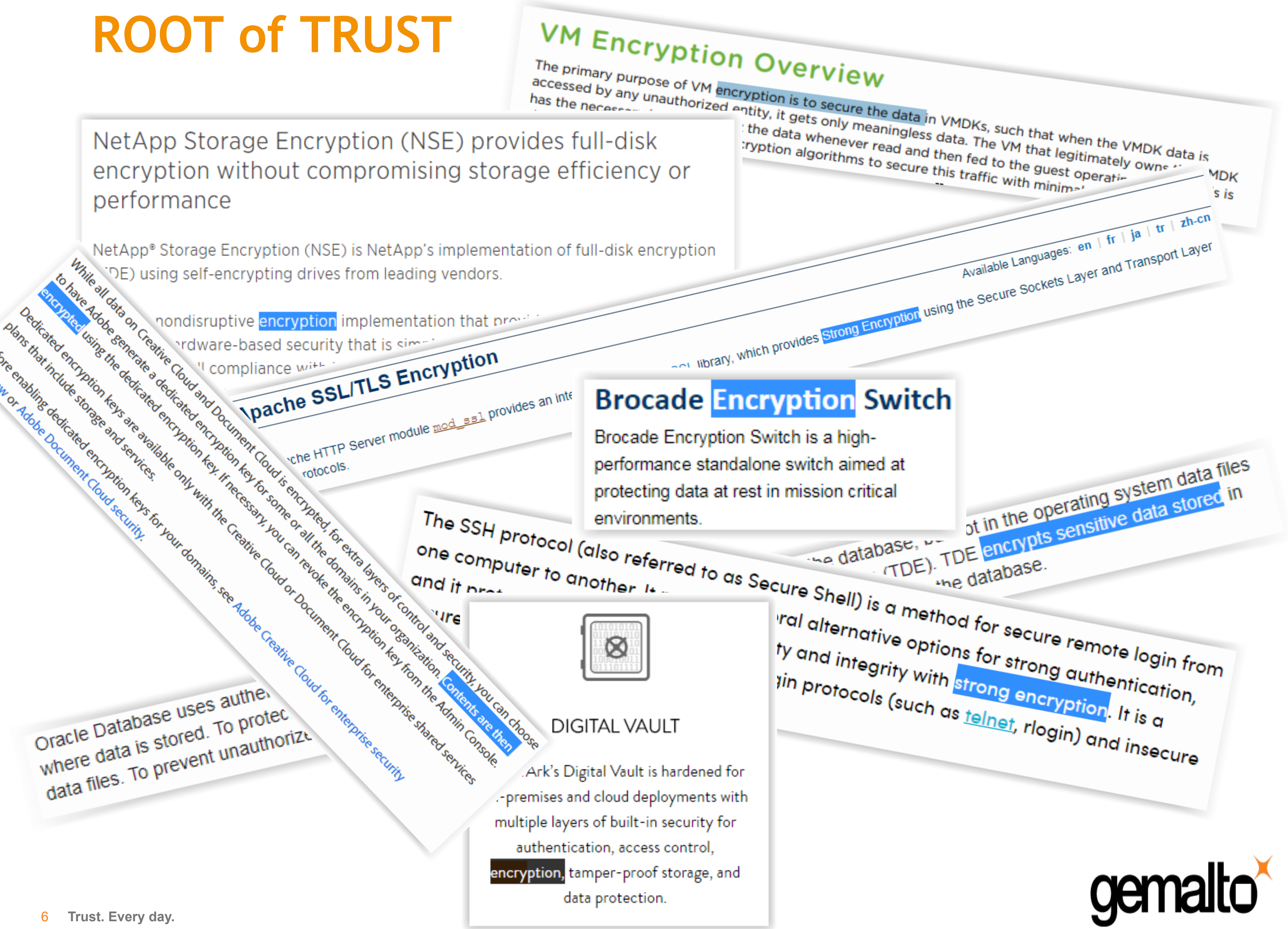
ROOT of TRUST

Zaufanie jest czynnikiem stabilizującym, pozwalającym się skoncentrować na istocie aktywności i jest doskonaleniu

ROOT of TRUST

gemalto

ROOT of TRUST



VM Encryption Overview

The primary purpose of VM encryption is to secure the data in VMDKs, such that when the VMDK data is
accessed by any unauthorized entity, it gets only meaningless data. The VM that legitimately owns
has the necess
the data whenever read and then fed to the guest operati
ryption algorithms to secure this traffic with minima
MDK
s is

NetApp Storage Encryption (NSE) provides full-disk encryption without compromising storage efficiency or performance

NetApp® Storage Encryption (NSE) is NetApp's implementation of full-disk encryption
DE) using self-encrypting drives from leading vendors.

nondisruptive encryption implementation that prov
rdware-based security that is sim
ll compliance with

Available Languages: en | fr | ja | tr | zh-cn

pache SSL/TLS Encryption

che HTTP Server module mod_ssl provides an inte
SSL library, which provides Strong Encryption using the Secure Sockets Layer and Transport Layer
rotocols.

While all data on Creative Cloud and Document Cloud is encrypted, for extra layers of control and security, you can choose
to have Adobe generate a dedicated encryption key for some or all the domains in your organization. Contents are then
encrypted using the dedicated encryption key. If necessary, you can revoke the encryption key from the Admin Console.
Dedicated encryption keys are available only with the Creative Cloud or Document Cloud for enterprise shared services
plans that include storage and services.
ore enabling dedicated encryption keys for your domains, see Adobe Creative Cloud for enterprise security
w or Adobe Document Cloud security.

Brocade Encryption Switch

Brocade Encryption Switch is a high-performance standalone switch aimed at protecting data at rest in mission critical environments.

pt in the operating system data files
e database,
(TDE). TDE encrypts sensitive data stored in
the database.

Oracle Database uses authe
where data is stored. To protec
data files. To prevent unauthorize

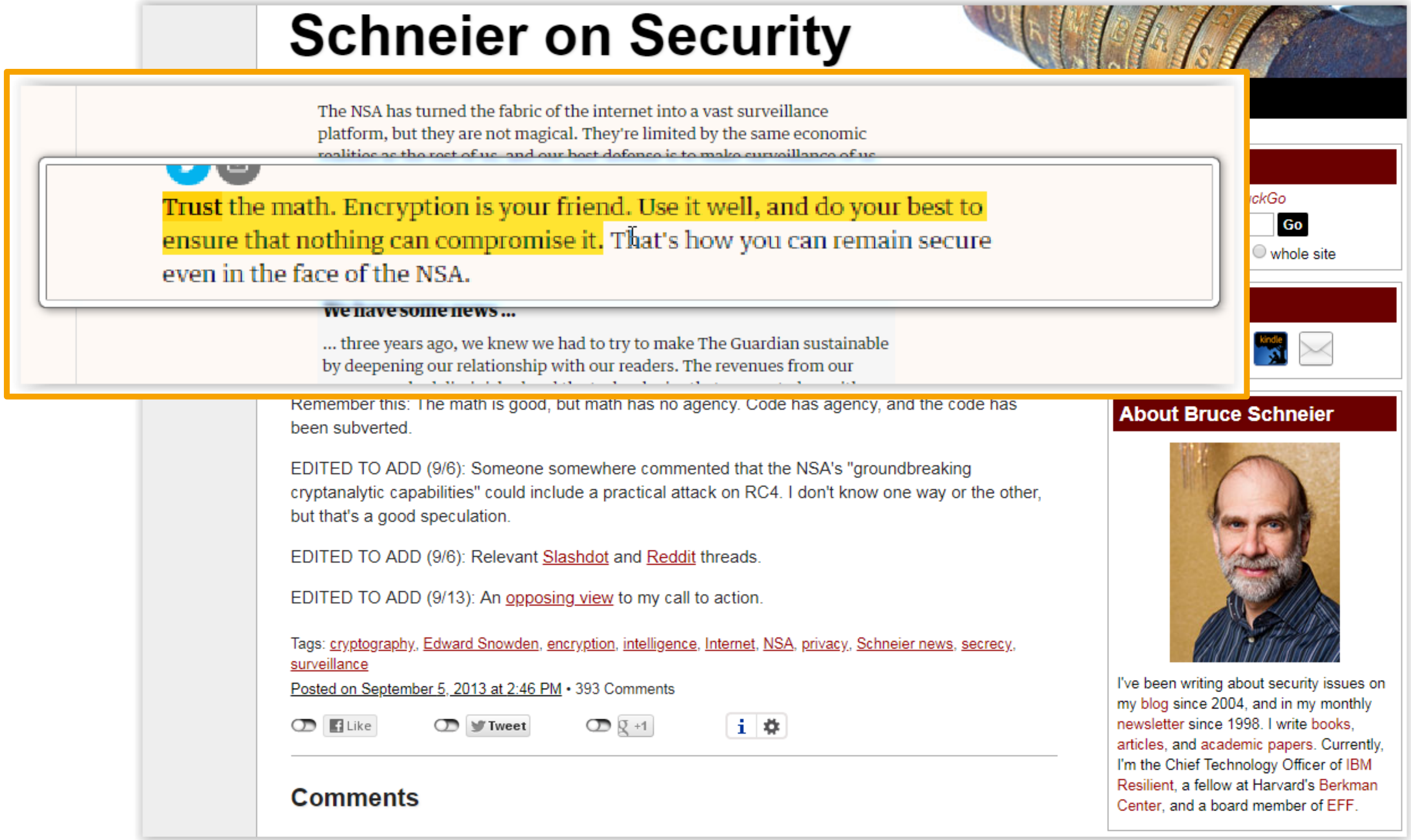
The SSH protocol (also referred to as Secure Shell) is a method for secure remote login from
one computer to another. It
and it prot
ure
ral alternative options for strong authentication,
ty and integrity with strong encryption. It is a
gin protocols (such as telnet, rlogin) and insecure

DIGITAL VAULT

Ark's Digital Vault is hardened for
-premises and cloud deployments with
multiple layers of built-in security for
authentication, access control,
encryption, tamper-proof storage, and
data protection.

gemalto

ROOT of TRUST



Schneier on Security

The NSA has turned the fabric of the internet into a vast surveillance platform, but they are not magical. They're limited by the same economic realities as the rest of us, and our best defence is to make surveillance of us

Trust the math. Encryption is your friend. Use it well, and do your best to ensure that nothing can compromise it. That's how you can remain secure even in the face of the NSA.

We have some news ...

... three years ago, we knew we had to try to make The Guardian sustainable by deepening our relationship with our readers. The revenues from our

Remember this: The math is good, but math has no agency. Code has agency, and the code has been subverted.

EDITED TO ADD (9/6): Someone somewhere commented that the NSA's "groundbreaking cryptanalytic capabilities" could include a practical attack on RC4. I don't know one way or the other, but that's a good speculation.

EDITED TO ADD (9/6): Relevant Slashdot and Reddit threads.

EDITED TO ADD (9/13): An opposing view to my call to action.

Tags: cryptography, Edward Snowden, encryption, intelligence, Internet, NSA, privacy, Schneier news, secrecy, surveillance

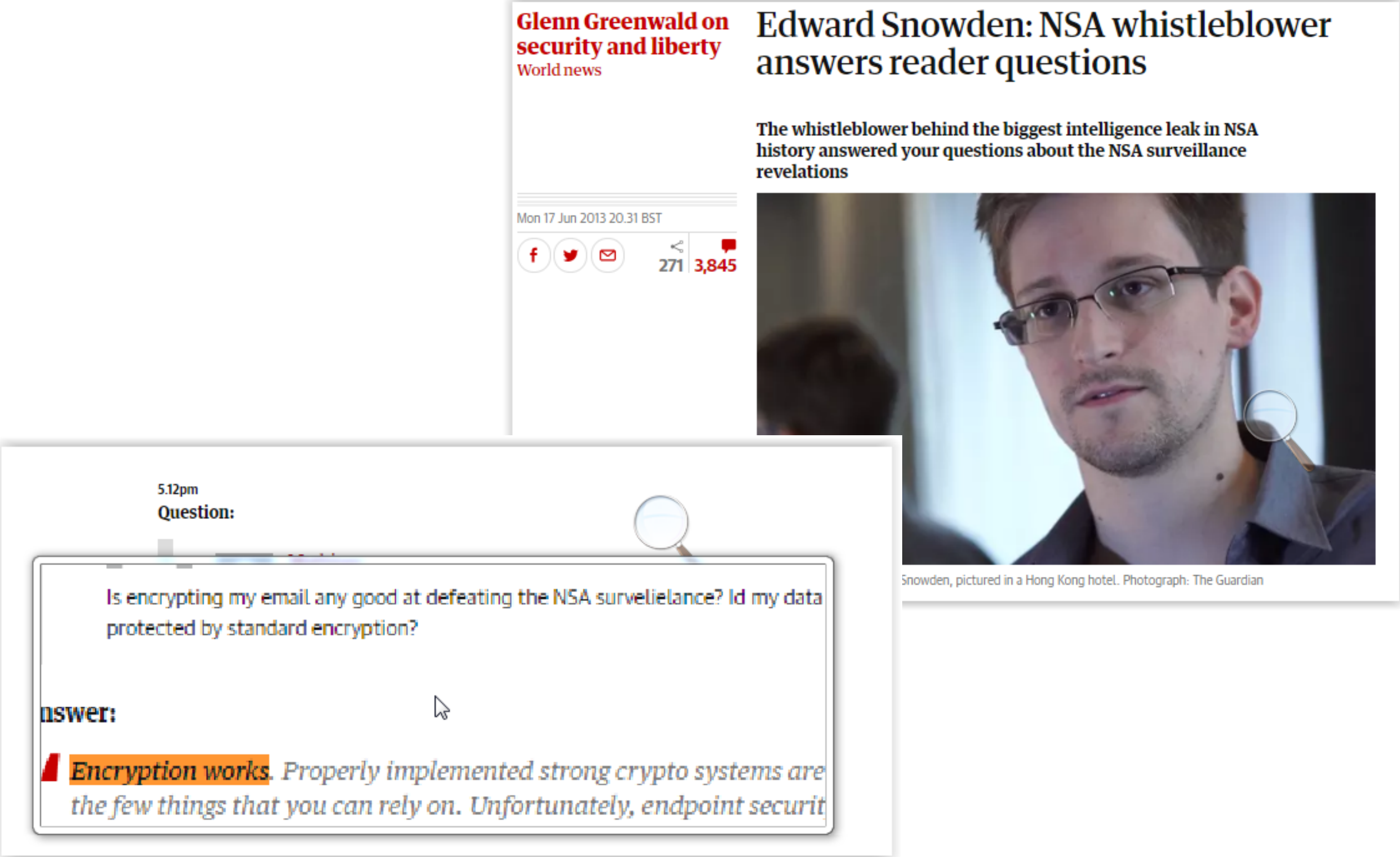
Posted on September 5, 2013 at 2:46 PM • 393 Comments

Comments

About Bruce Schneier

I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I write books, articles, and academic papers. Currently, I'm the Chief Technology Officer of IBM Resilient, a fellow at Harvard's Berkman Center, and a board member of EFF.

ROOT of TRUST



Glenn Greenwald on security and liberty
World news

Mon 17 Jun 2013 20.31 BST

Edward Snowden: NSA whistleblower answers reader questions

The whistleblower behind the biggest intelligence leak in NSA history answered your questions about the NSA surveillance revelations

Snowden, pictured in a Hong Kong hotel. Photograph: The Guardian

5.12pm
Question:

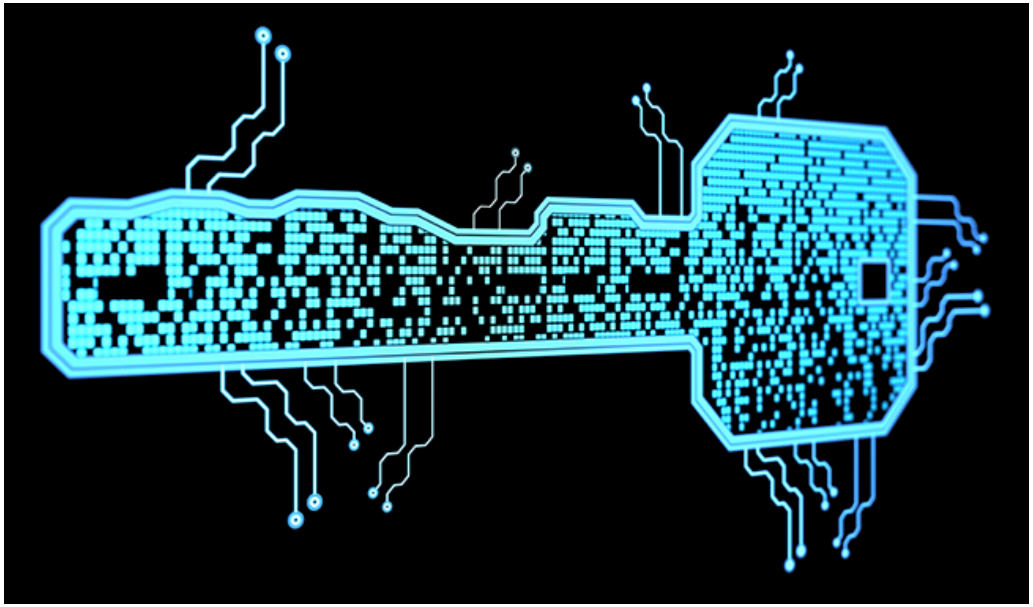
Is encrypting my email any good at defeating the NSA survelielance? Id my data protected by standard encryption?

nswer:

Encryption works. Properly implemented strong crypto systems are the few things that you can rely on. Unfortunately, endpoint securit

ROOT of TRUST

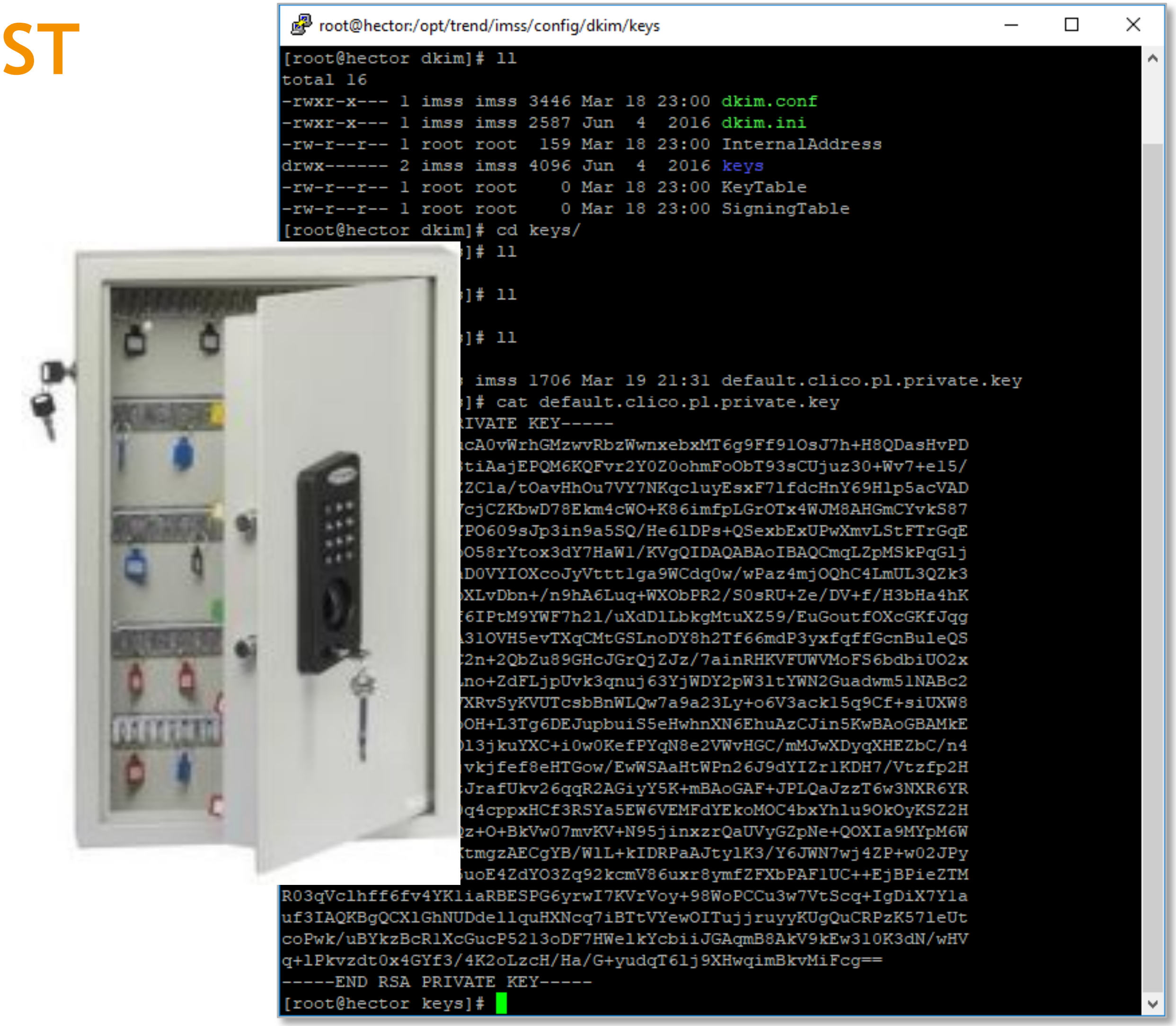
co jest najważniejsze w kryptografi?



ROOT of TRUST

czy wiesz gdzie są Twoje klucze i jak są przechowywane?

ROOT of TRUST



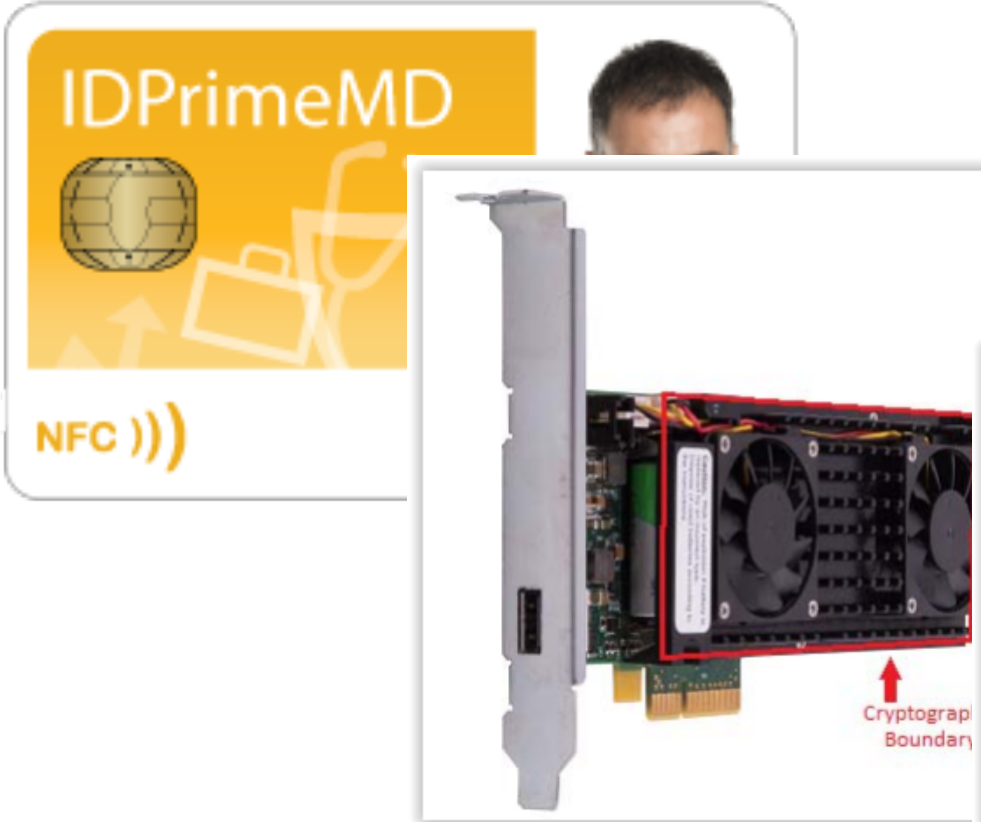
```
[root@hector dkim]# ll
total 16
-rwxr-x--- 1 imss imss 3446 Mar 18 23:00 dkim.conf
-rwxr-x--- 1 imss imss 2587 Jun  4  2016 dkim.ini
-rw-r--r-- 1 root root  159 Mar 18 23:00 InternalAddress
drwx------ 2 imss imss 4096 Jun  4  2016 keys
-rw-r--r-- 1 root root    0 Mar 18 23:00 KeyTable
-rw-r--r-- 1 root root    0 Mar 18 23:00 SigningTable
[root@hector dkim]# cd keys/
                 ]# ll

                 ]# ll

                 ]# ll

                   imss 1706 Mar 19 21:31 default.clico.pl.private.key
                 ]# cat default.clico.pl.private.key
                 RIVATE KEY-----
                 cA0vWrhGMzwvRbzWwnxebxMT6g9Ff91OsJ7h+H8QDasHvPD
                 tiAajEPQM6KQFvr2Y0Z0ohmFoObT93sCUjuz30+Wv7+e15/
                 ZCla/tOavHhOu7VY7NKqcluyEsxF7lfdcHnY69Hlp5acVAD
                 cjCZKbwD78Ekm4cWO+K86imfpLGrOTx4WJM8AHGmCYvkS87
                 PO609sJp3in9a5SQ/He61DPs+QSexbExUPwXmvLStFTrGqE
                 O58rYtox3dY7HaW1/KVgQIDAQABAoIBAQCmqLZpMSkPqG1j
                 D0VYIOXcoJyVtttlga9WCdq0w/wPaz4mjOQhC4LmUL3QZk3
                 XLvDbn+/n9hA6Luq+WXObPR2/S0sRU+Ze/DV+f/H3bHa4hK
                 6IPtM9YWF7h21/uXdDlLbkgMtuXZ59/EuGoutfOXcGKfJqg
                 31OVH5evTXqCMtGSLnoDY8h2Tf66mdP3yxfqffGcnBuleQS
                 2n+2QbZu89GHcJGrQjZJz/7ainRHKVFUWVMoFS6bdbiUO2x
                 no+ZdFLjpUvk3qnuj63YjWDY2pW31tYWN2Guadwm51NABc2
                 XRvSyKVUTcsbBnWLQw7a9a23Ly+o6V3ack15q9Cf+siUXW8
                 OH+L3Tg6DEJupbuiS5eHwhnXN6EhuAzCJin5KwBAoGBAMkE
                 13jkuYXC+i0w0KefPYqN8e2VWvHGC/mMJwXDyqXHEZbC/n4
                 vkjfef8eHTGow/EwWSAaHtWPn26J9dYIZr1KDH7/Vtzfp2H
                 JrafUkv26qqR2AGiyY5K+mBAoGAF+JPLQaJzzT6w3NXR6YR
                 q4cppxHCf3RSYa5EW6VEMFdYEkoMOC4bxYhlu9OkOyKSZ2H
                 z+O+BkVw07mvKV+N95jinxzrQaUVyGZpNe+QOXIa9MYpM6W
                 tmgzAECgYB/W1L+kIDRPaAJty1K3/Y6JWN7wj4ZP+w02JPy
                 uoE4ZdYO3Zq92kcmV86uxr8ymfZFXbPAF1UC++EjBPieZTM
R03qVclhff6fv4YKliaRBESPG6yrwI7KVrVoy+98WoPCCu3w7VtScq+IgDiX7Yla
uf3IAQKBgQCXlGhNUDdellquHXNcq7iBTtVYewOITujjruyyKUgQuCRPzK57leUt
coPwk/uBYkzBcRlXcGucP5213oDF7HWelkYcbiiJGAqmB8AkV9kEw310K3dN/wHV
q+lPkvzdt0x4GYf3/4K2oLzcH/Ha/G+yudqT61j9XHwqimBkvMiFcg==
-----END RSA PRIVATE KEY-----
[root@hector keys]#
```

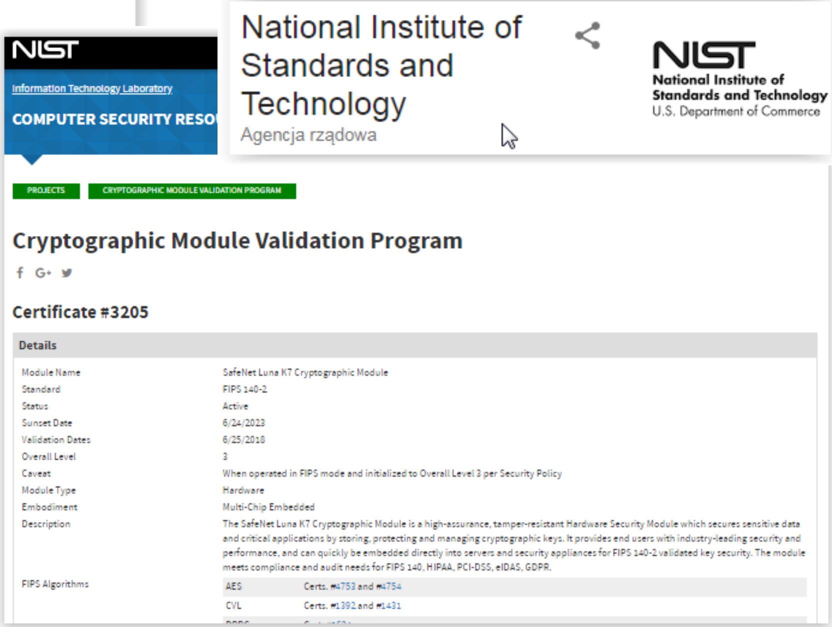
czas najwyższy coś z tym zrobić…

ROOT of TRUST

H S M

Hardware Security Module




NIST
Information Technology Laboratory
COMPUTER SECURITY RESO
PROJECTS
CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

National Institute of Standards and Technology

Agencja rządowa

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Cryptographic Module Validation Program

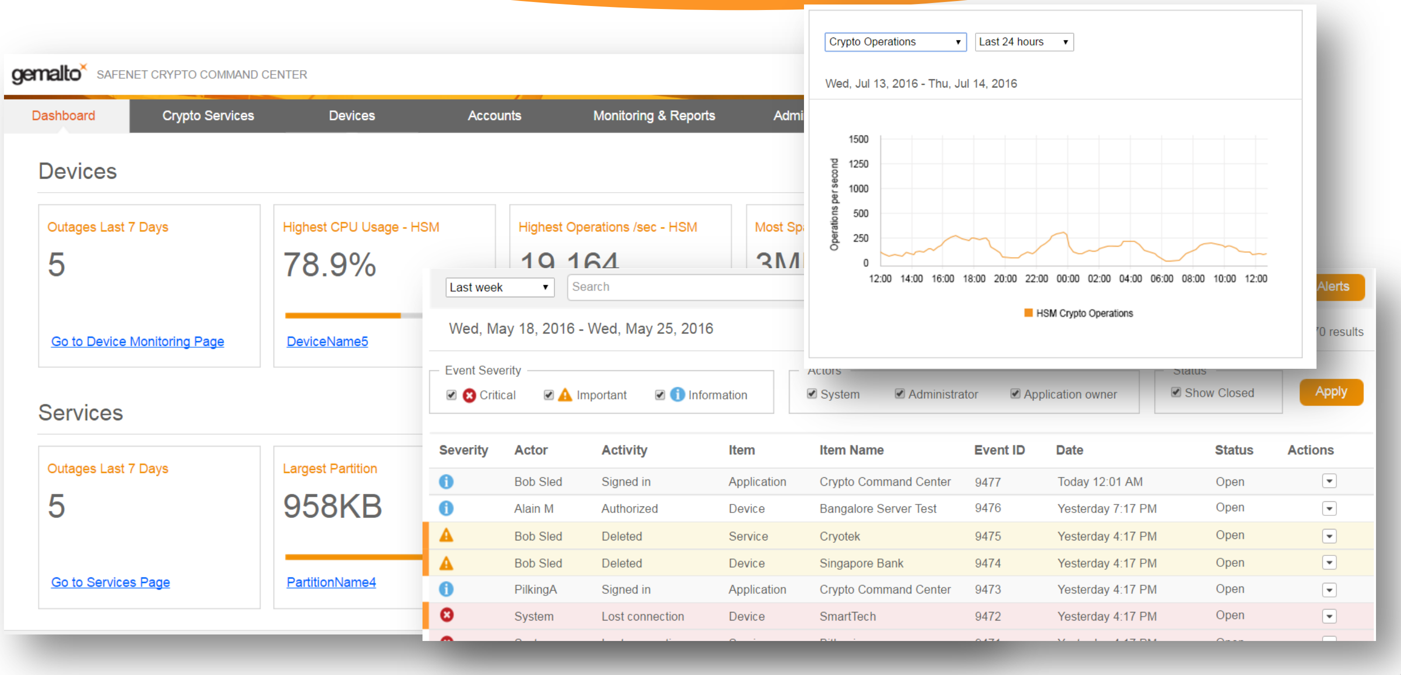
Certificate #3205

Details	
Module Name	SafeNet Luna K7 Cryptographic Module
Standard	FIPS 140-2
Status	Active
Sunset Date	6/24/2023
Validation Dates	6/25/2018
Overall Level	3
Caveat	When operated in FIPS mode and initialized to Overall Level 3 per Security Policy
Module Type	Hardware
Embodiment	Multi-Chip Embedded
Description	The SafeNet Luna K7 Cryptographic Module is a high-assurance, tamper-resistant Hardware Security Module which secures sensitive data and critical applications by storing, protecting and managing cryptographic keys. It provides end users with industry-leading security and performance, and can quickly be embedded directly into servers and security appliances for FIPS 140-2 validated key security. The module meets compliance and audit needs for FIPS 140, HIPAA, PCI-DSS, eIDAS, GDPR.
FIPS Algorithms	AES Certs. #4753 and #4754
	CVL Certs. #1392 and #1431

ROOT of TRUST

SafeNet Network HSM

SafeNet PCIe HSM



gemalto SAFENET CRYPTO COMMAND CENTER

Devices

Outages Last 7 Days	Highest CPU Usage - HSM	Highest Operations /sec - HSM	Most Sp
5	78.9%	19,164	3M
Go to Device Monitoring Page	DeviceName5		

Services

Outages Last 7 Days	Largest Partition
5	958KB
Go to Services Page	PartitionName4

Crypto Operations ▾ Last 24 hours ▾

Wed, Jul 13, 2016 - Thu, Jul 14, 2016

Last week ▾ Search

Alerts

Wed, May 18, 2016 - Wed, May 25, 2016

0 results

Event Severity: ☑ ✖ Critical ☑ ⚠ Important ☑ ℹ Information

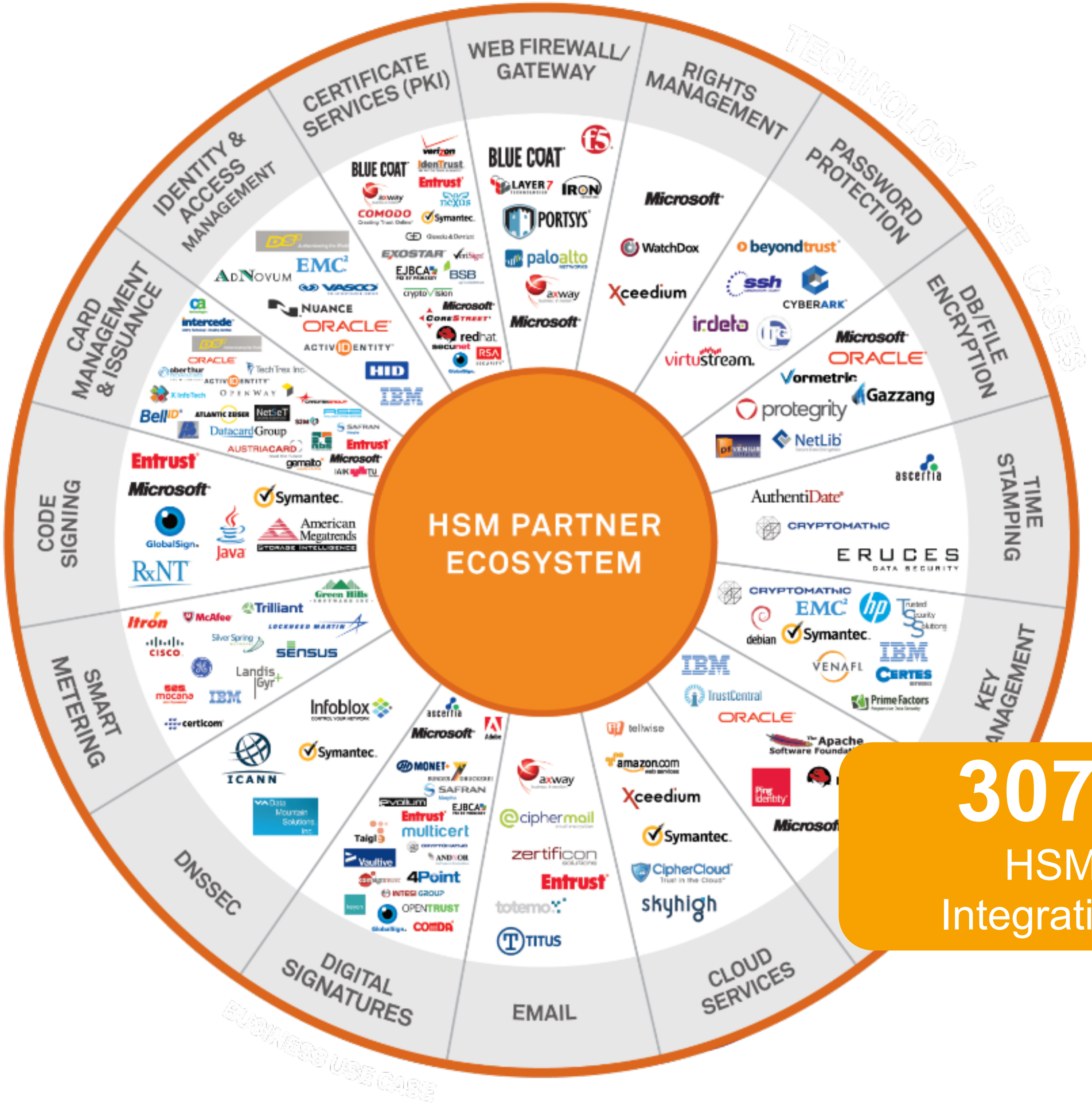
Actors: ☑ System ☑ Administrator ☑ Application owner

Status: ☑ Show Closed

Apply

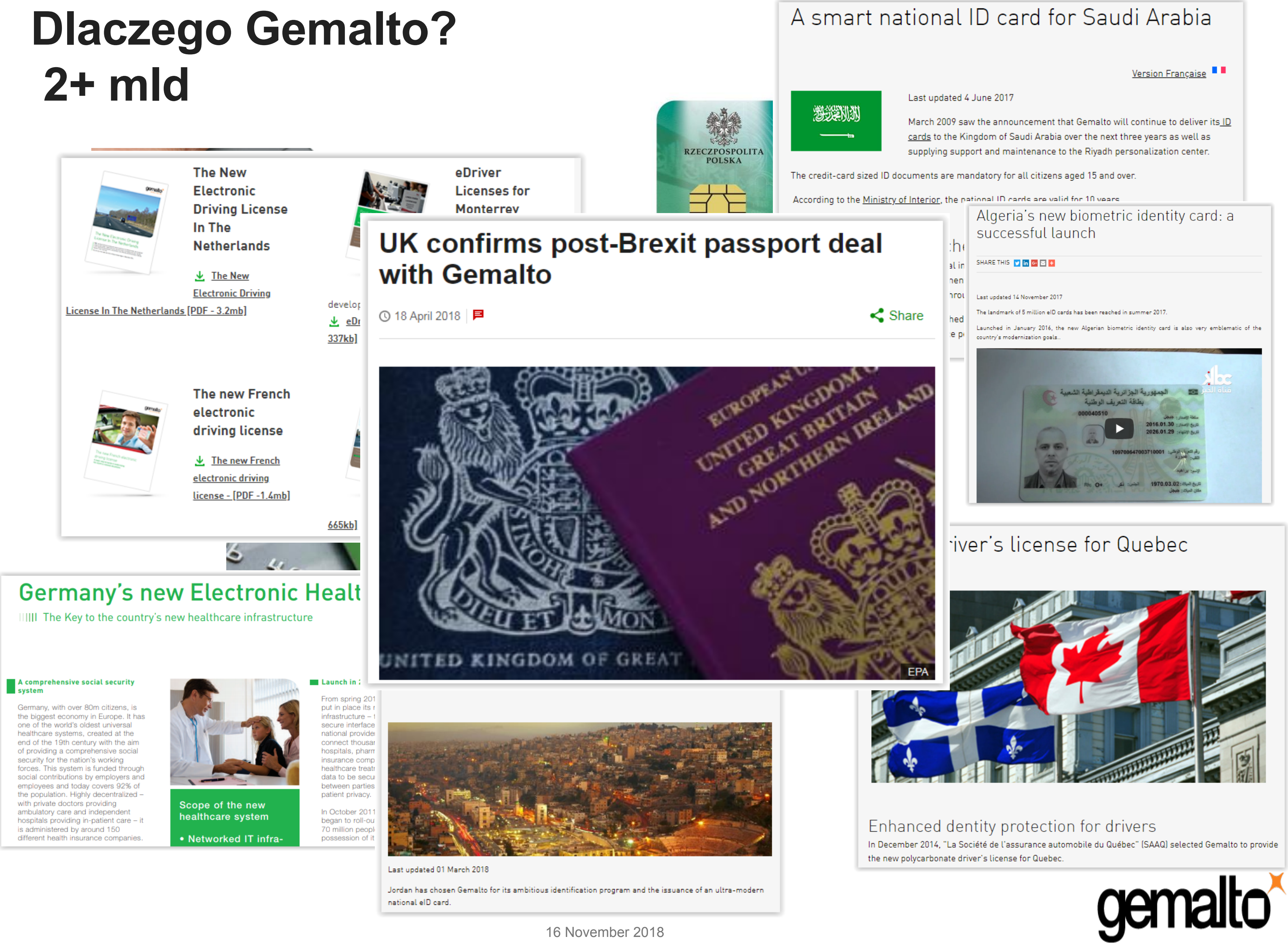
Severity	Actor	Activity	Item	Item Name	Event ID	Date	Status	Actions
ℹ	Bob Sled	Signed in	Application	Crypto Command Center	9477	Today 12:01 AM	Open	▾
ℹ	Alain M	Authorized	Device	Bangalore Server Test	9476	Yesterday 7:17 PM	Open	▾
⚠	Bob Sled	Deleted	Service	Cryotek	9475	Yesterday 4:17 PM	Open	▾
⚠	Bob Sled	Deleted	Device	Singapore Bank	9474	Yesterday 4:17 PM	Open	▾
ℹ	PilkingA	Signed in	Application	Crypto Command Center	9473	Yesterday 4:17 PM	Open	▾
✖	System	Lost connection	Device	SmartTech	9472	Yesterday 4:17 PM	Open	▾

ROOT of TRUST



307+
HSM
Integrations

Dlaczego Gemalto?
2+ mld



A smart national ID card for Saudi Arabia

Version Française

Last updated 4 June 2017

March 2009 saw the announcement that Gemalto will continue to deliver its ID cards to the Kingdom of Saudi Arabia over the next three years as well as supplying support and maintenance to the Riyadh personalization center.

The credit-card sized ID documents are mandatory for all citizens aged 15 and over.

According to the Ministry of Interior, the national ID cards are valid for 10 years

The New Electronic Driving License In The Netherlands

The New Electronic Driving License In The Netherlands [PDF - 3.2mb]

eDriver Licenses for Monterrey

develop

eDr

337kb]

The new French electronic driving license

The new French electronic driving license - [PDF -1.4mb]

665kb]

UK confirms post-Brexit passport deal with Gemalto

18 April 2018

Share

Algeria's new biometric identity card: a successful launch

SHARE THIS

Last updated 14 November 2017

The landmark of 5 million eID cards has been reached in summer 2017.

Launched in January 2016, the new Algerian biometric identity card is also very emblematic of the country's modernization goals..

Germany's new Electronic Healt

The Key to the country's new healthcare infrastructure

A comprehensive social security system

Germany, with over 80m citizens, is the biggest economy in Europe. It has one of the world's oldest universal healthcare systems, created at the end of the 19th century with the aim of providing a comprehensive social security for the nation's working forces. This system is funded through social contributions by employers and employees and today covers 92% of the population. Highly decentralized – with private doctors providing ambulatory care and independent hospitals providing in-patient care – it is administered by around 150 different health insurance companies.

Scope of the new healthcare system

- Networked IT infra-

Launch in 2

From spring 201 put in place its r infrastructure – t secure interface national provider connect thousar hospitals, pharm insurance comp healthcare treatr data to be secur between parties patient privacy.

In October 2011 began to roll-ou 70 million peopl possession of it

Last updated 01 March 2018

Jordan has chosen Gemalto for its ambitious identification program and the issuance of an ultra-modern national eID card.

river's license for Quebec

Enhanced dentity protection for drivers

In December 2014, "La Société de l'assurance automobile du Québec" (SAAQ) selected Gemalto to provide the new polycarbonate driver's license for Quebec.

16 November 2018

ROOT of TRUST

gemalto
security to be free

Dziękuję!!!
Piotr.Wrobel@gemalto.com