

**Vlastimil Klíma and Martin Baroš**



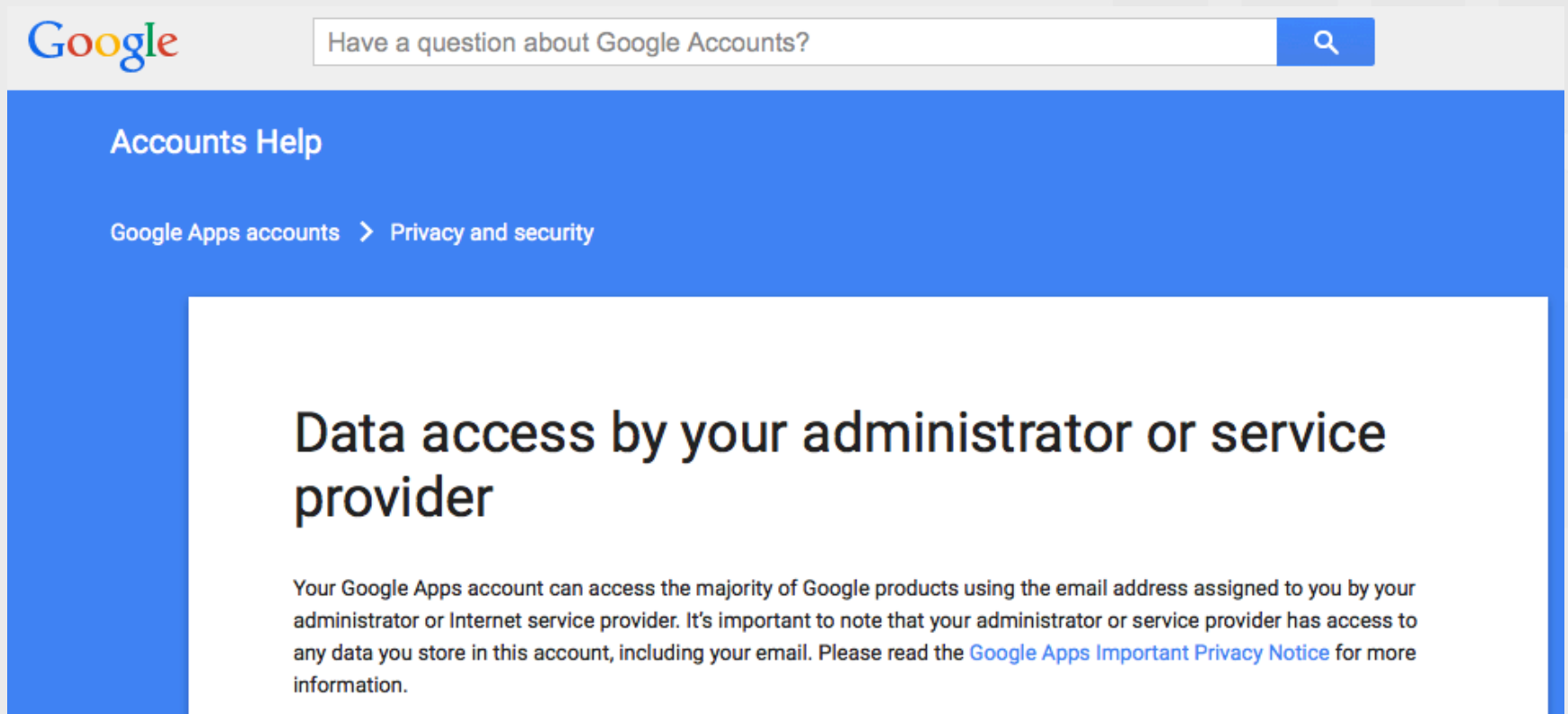
---

# **Data Protection in the Cloud**



# Let's move to the cloud - it's trendy!

Does using cloud services  
= a loss of control over my data?

A screenshot of the Google Accounts Help page. The top section has a blue header with the Google logo on the left, a search bar in the center containing the text "Have a question about Google Accounts?", and a magnifying glass icon on the right. Below the header, the page title "Accounts Help" is displayed. A breadcrumb trail shows "Google Apps accounts" followed by a right-pointing chevron and "Privacy and security". The main content area has a white background and features the heading "Data access by your administrator or service provider". Below this heading, a paragraph explains that a Google Apps account can access most Google products using an email address assigned by an administrator or Internet service provider, and notes that the administrator or service provider has access to any data stored in the account, including email. It concludes by directing the user to read the "Google Apps Important Privacy Notice" for more information.

Google

Have a question about Google Accounts?

Accounts Help

Google Apps accounts > Privacy and security

## Data access by your administrator or service provider

Your Google Apps account can access the majority of Google products using the email address assigned to you by your administrator or Internet service provider. It's important to note that your administrator or service provider has access to any data you store in this account, including your email. Please read the [Google Apps Important Privacy Notice](#) for more information.

# **Provider has access to your data**

**It's important to note that your administrator or service provider has access to any data you store in an account, including your email.**



# Cryptography and its Implementation

- ① Perfectly encrypted cloud storage  
from a cryptographic perspective
- ② Perfectly encrypted cloud storage  
from a implementation perspective



①

# Perfectly Encrypted Cloud Storage from a Cryptographic Perspective



# Cloud Solutions Under Scrutiny



# Perfect Cloud Storage Conditions

## [from cryptografic point of view ]

1. End-to-end encryption
2. Client-side key generation
3. User-friendly interface
4. Data sharing is truly secure and easy
5. Top Secret security level encryption algorithms
6. All data on the server is encrypted as well



# 1. End-to-End Encryption

- A. client-side encryption/  
decryption of data
- B. encrypted and authenticated  
channel for transferring data  
to the server





# E2E encryption vs. Google drive

A. client-side encryption/  
decryption of data

- client-server encryption only

B. encrypted channel  
for transferring data  
to the server

- https



## 2. Client-Side Key Generation

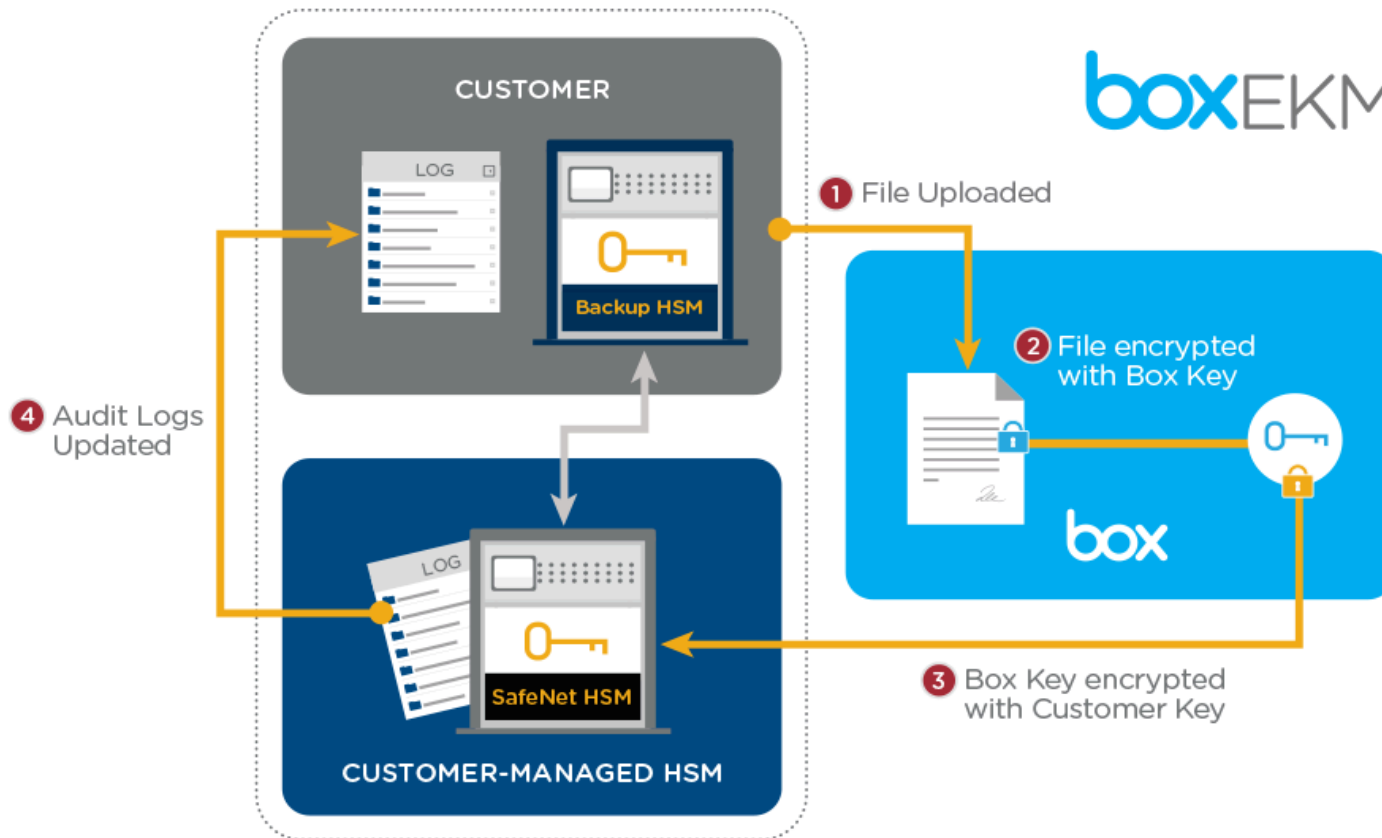
- A. includes entropy generation
- B. Keys are never stored on the server
- C. optimal physical separation of keys from the data



# Key Generation vs. Box



keys are generated on the server



# **3. User-Friendly Interface**

**A. no knowledge of encryption necessary**

**B. easy to store**

**C. easy to share**



## **4. Data Sharing must be Truly Secure and Easy**

**A. the process of sharing does not  
require expert knowledge**

**B. sharing does not weaken the  
protection of data**



# sharing vs. spider oak

zero-knowledge loss while sharing

*“... ShareRoom is not Zero-Knowledge ...”*



Secure Backup



Sync Anywhere



Share Privately

# **5. Cryptographic functions on maximum security level**

**A. Algorithms approved by NSA  
for Top Secret data protection  
(AES-256, EC P-384)**



## **6. All Valuable Information must be Encrypted**

**A. file and directory names**

**B. file authors and recipients  
of shared files**

**C. file directory structure**





# **All Information Encryption vs. Wuala**


**“Upward Inheritance of Access Rights”  
- white paper Cryptree**



# attack ready approach is essential

“16 vulnerabilities in debian in 2014”

- National Vulnerability Database



The screenshot shows the NVD website header with the DHS/US-CERT logo and NIST logo. The main title is "National Vulnerability Database" with the tagline "automating vulnerability management, security measurement, and compliance checking". Below the header is a navigation bar with links: Vulnerabilities, Checklists, 800-53/800-53A, Product Dictionary, Home, SCAP, SCAP Validated Tools, and SCAP Events. The main content area is divided into two sections: "Mission and Overview" and "Search Results (Refine Search)".

**National Vulnerability Database**  
automating vulnerability management, security measurement, and compliance checking

**Vulnerabilities** | **Checklists** | **800-53/800-53A** | **Product Dictionary**

**Home** | **SCAP** | **SCAP Validated Tools** | **SCAP Events**

**Mission and Overview**

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability

**Search Results ([Refine Search](#))**

There are **16** matching records.

**Search Parameters:**

- **Contains Software Flaws (CVE)**
- **CPE Vendor:** cpe:/:debian
- **CPE Product:** cpe/::debian\_linux
- **Publication End Date:** 12/2014

②

# **Perfectly Encrypted Cloud Storage from a Implementation Perspective**



# **Perfect cloud storage premisses [from technologic point of view]**

**Connect anywhere**



# Perfect cloud storage premisses [from technologic point of view ]

Native lang for mobile + java for desktop

- Android, iOS, Windows = 99,1
- Windows, Mac OS, Linux

HTML 5 + CSS + JavaScript

- supported by web browsers
- supported by mobile devices



# Desktop browser performance

Google Chrome vs. Mozilla Firefox  
tested algorithms:

- AES-256
- EC (DH, shared secret, sign, verify)
- PBKDF2

Browser	Speed
Chrome	Identical
Firefox	



# Native language vs. JavaScript

Objective C vs. JavaScript (1 MB data file)  
on iPad Air

	JavaScript	Objective C	JavaScript / Objective C
AES-256 ENC	8 228 ms	30 ms	274
AES-256 DEC	9 126 ms	30 ms	304



# Cryptography in JavaScript

JavaScript encryption in web browser  
(50 KB data file, time: [ms])

	Ipad 2	Ipad Air 2	HTC One	Iphone 5S
AES-256 ENC	401	174	192	236





# Implementation conclusions

	Mobile devices Native language	Mobile devices JavaScript	Desktop JavaScript
Chat service	YES	YES	YES
Small files (<1 MB)	YES	YES	YES
Bigger files (photos)	YES	NO	YES



# Perfect cloud conclusion

- Defined 6 premises
- Suitable technology is available
- No product that reach this level of security
- Implemented proof of concept – Cryptelo Drive



# Thank you for your attention



---

**Vlastimil Klíma**

v.klima@volny.cz

**Martin Baroš**

baros@cryptelo.com



**[www.cryptelo.com/Lab](http://www.cryptelo.com/Lab)**