ShieldMyfiles

Encryption ≠ Protection

A proposed framework for thinking about file security

Joseph Webster, CISSP
Senior Member IEEE
BSEE Colorado State University
Software and Systems Security Architect
Founding member of ShieldMyfiles

June 9th, 2015

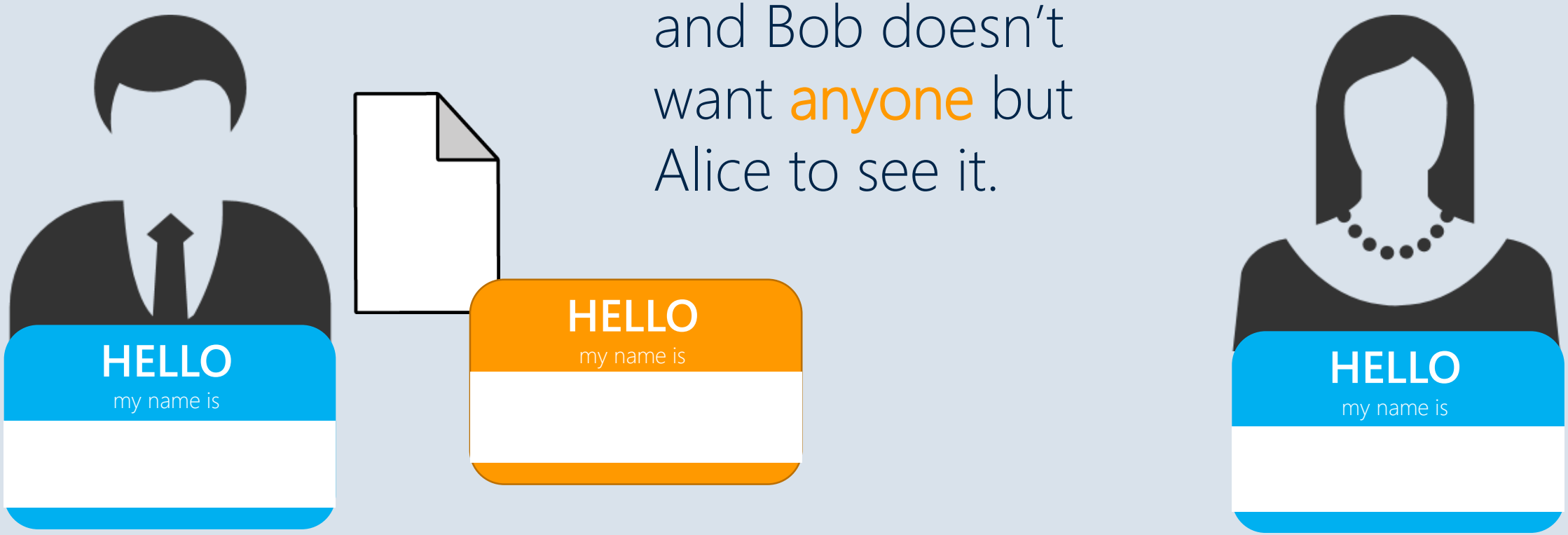
ShieldMyfiles

Introduction 1.0

Alice Needs Bob's File.

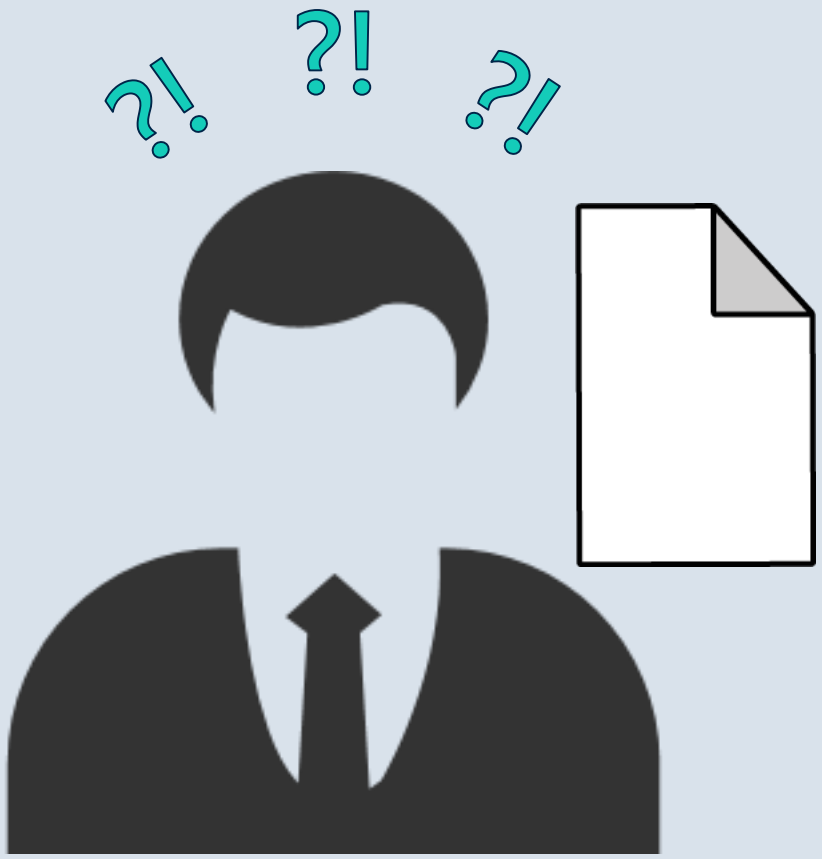
But...

Bob's file is sensitive and Bob doesn't want anyone but Alice to see it.



Introduction 1.1

Bob Has Some Concerns…

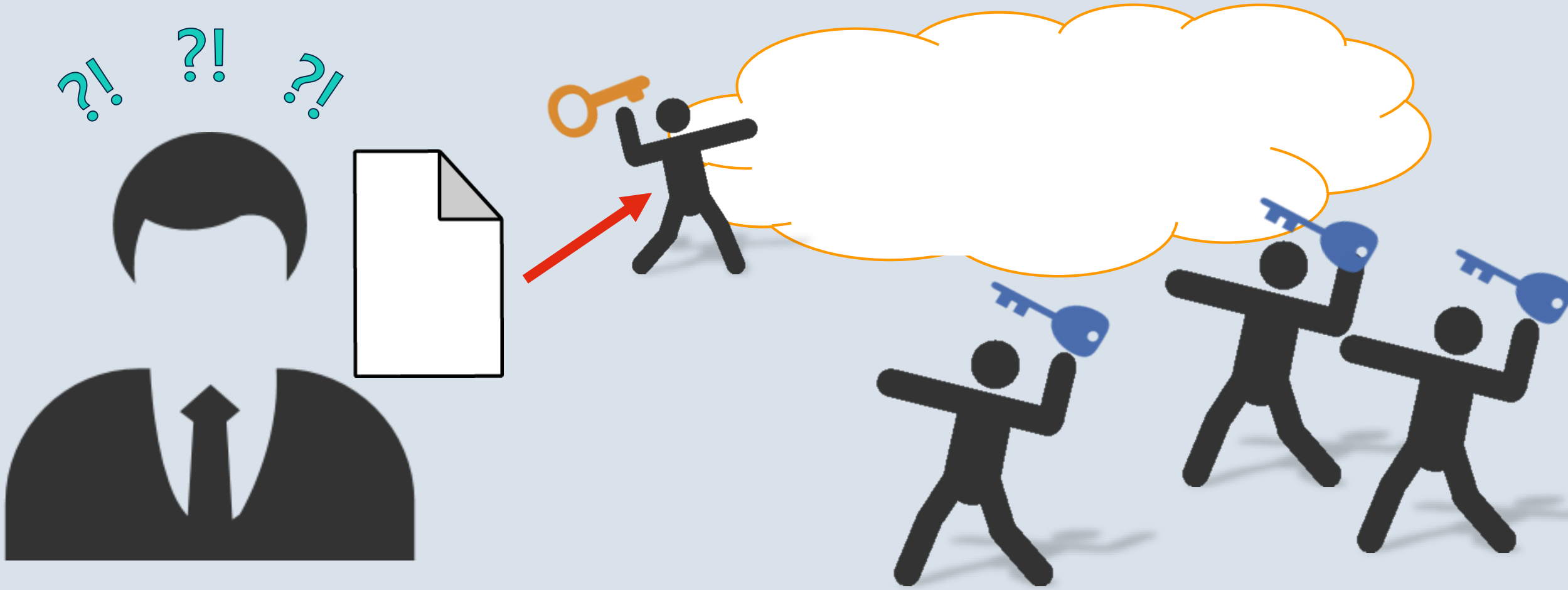


Bob fears for the Security of his files in the cloud

After All Bob Doesn't Control His Cloud

Introduction 1.1

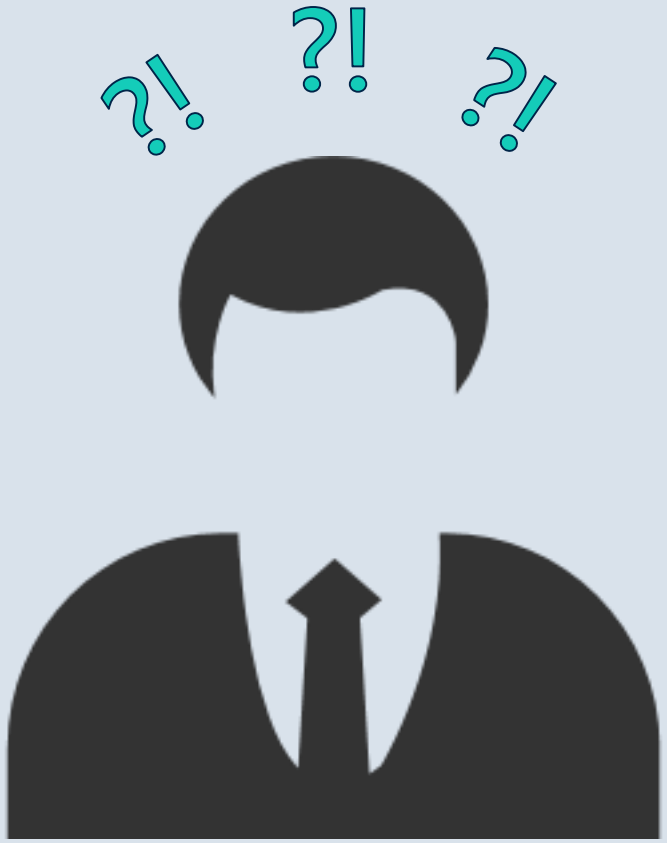
Bob Doesn't Want to Exchange Keys or Certificates …



ShieldMyfiles

Login Vignette Production Slide

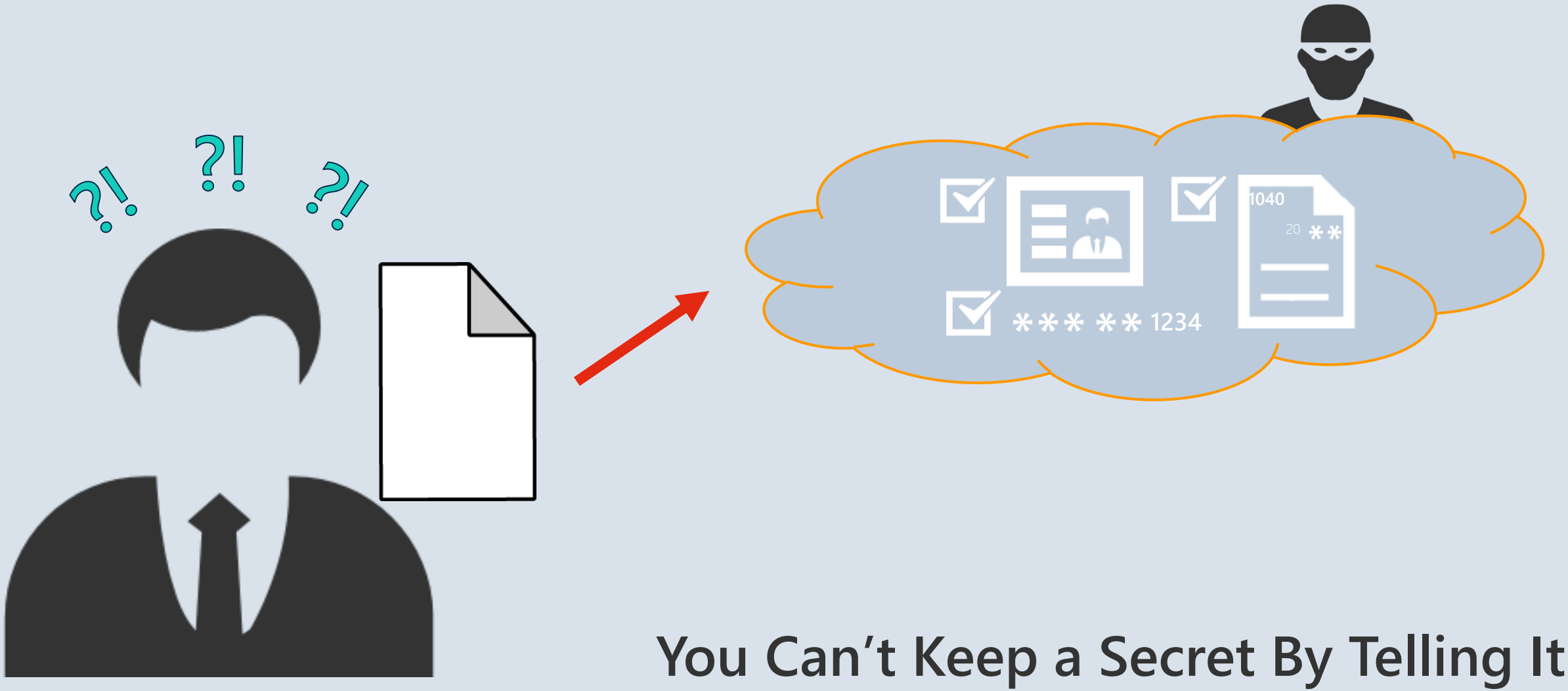
Bob Doesn't Have Time to Manage a Million User Accounts!



It Shouldn't Take a Portal to Share a Single File!

ShieldMyfiles

Introduction 1.1



You Can’t Keep a Secret By Telling It!

There are 3 Tenets to this Framework:

1) **Obfuscation**
2) **Access Controls**
   - Who
   - How
   - When
   - Where

   Files may be accessed
3) **Auditability**

Requiring Separation of Duties

ShieldMyfiles

Obfuscation

Obfuscation = Custody

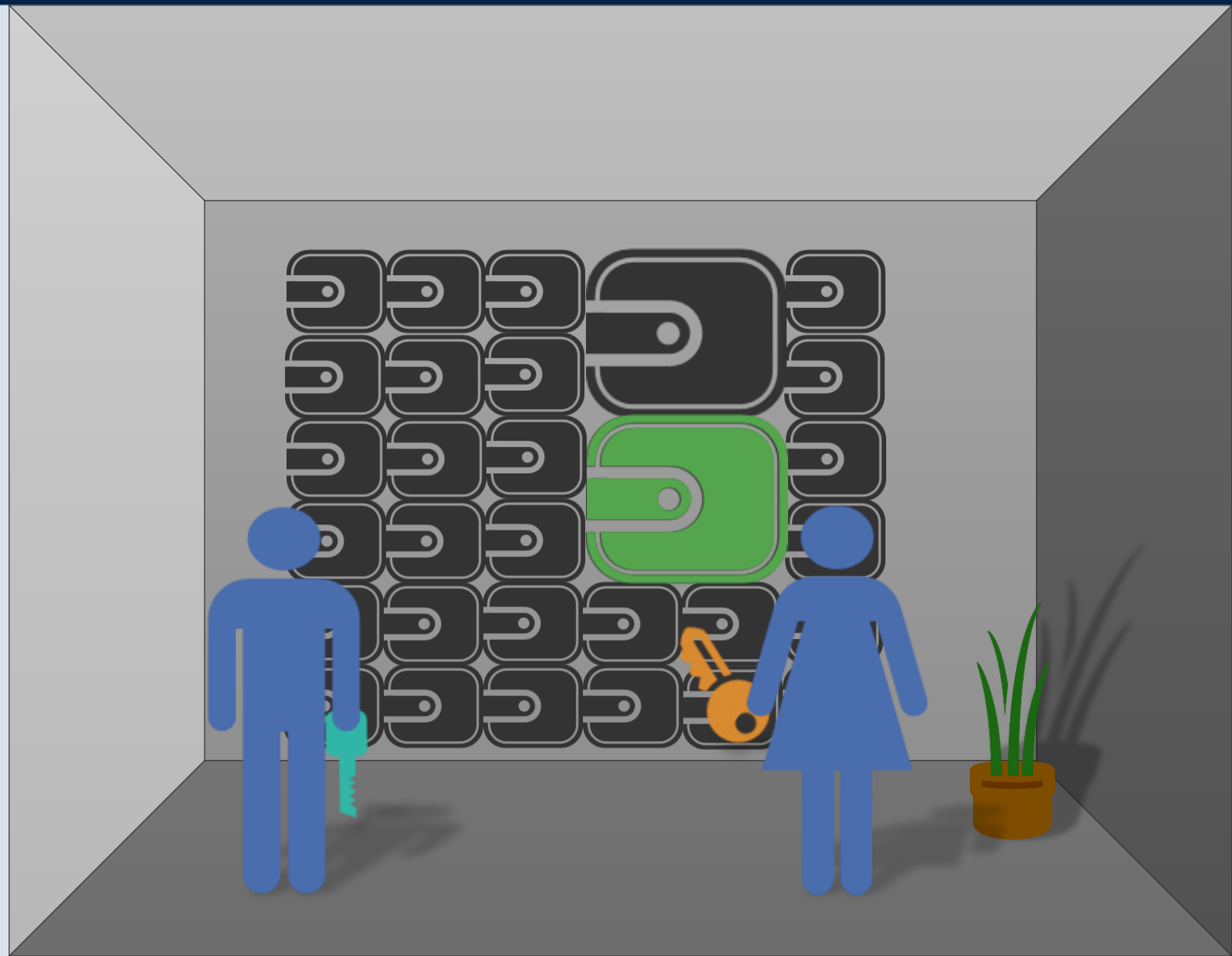
- **Protection without Possession**

Physical World

- Bank
- Safety Deposit Box

Digital World

- Encryption
- Enciphering
- Steganography



ShieldMyfiles

Access Controls

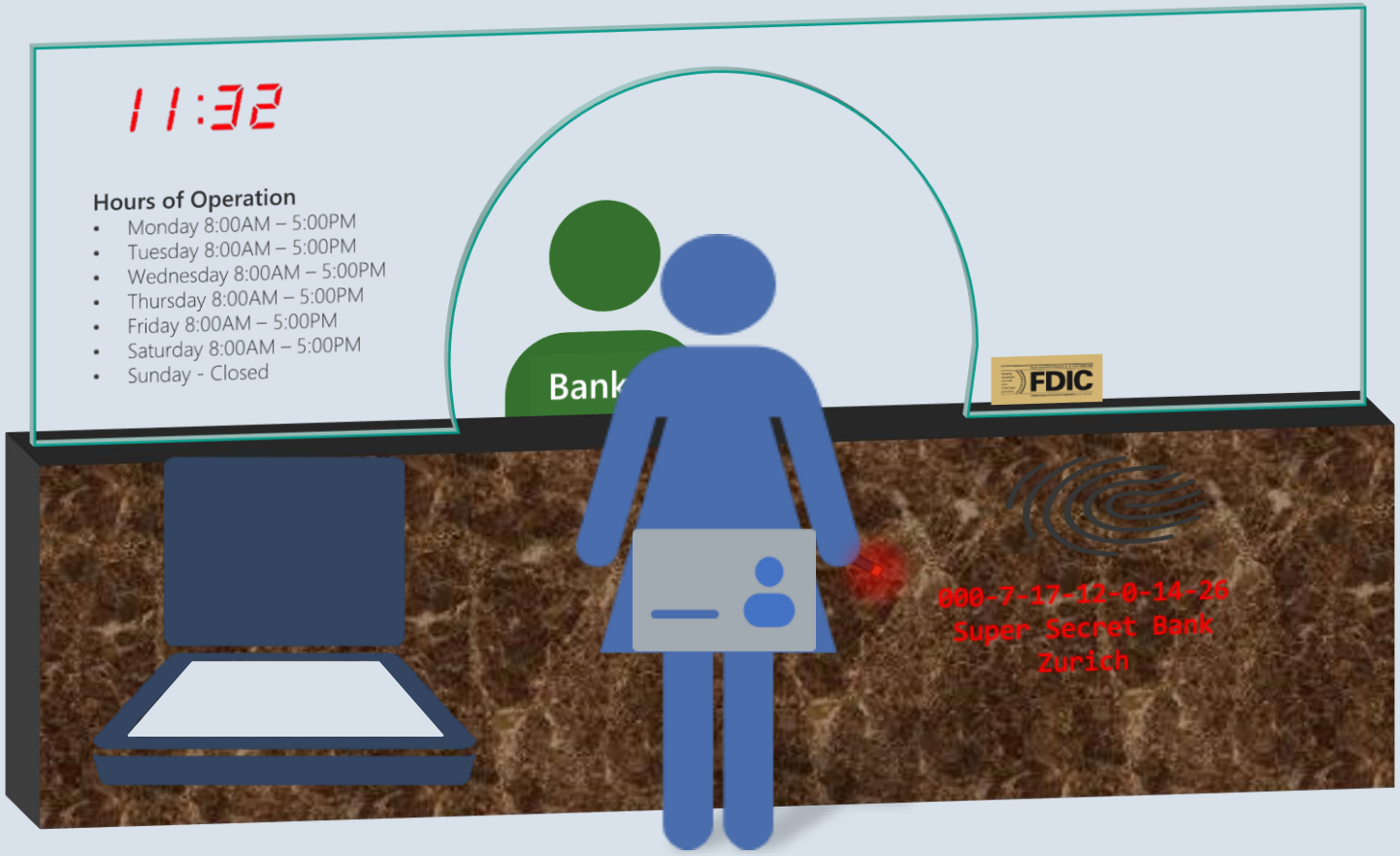
Access Controls = Authorization

Physical World - Bank

- Physical Location
- Hours of Operation
- Finger Print
- Signature Card
- Account Number

Digital World

- Where – Geolocation
- When – Expiration
- Who – Biometrics
- Who – Password
- How – UserID



Auditability

Auditability = Auditability

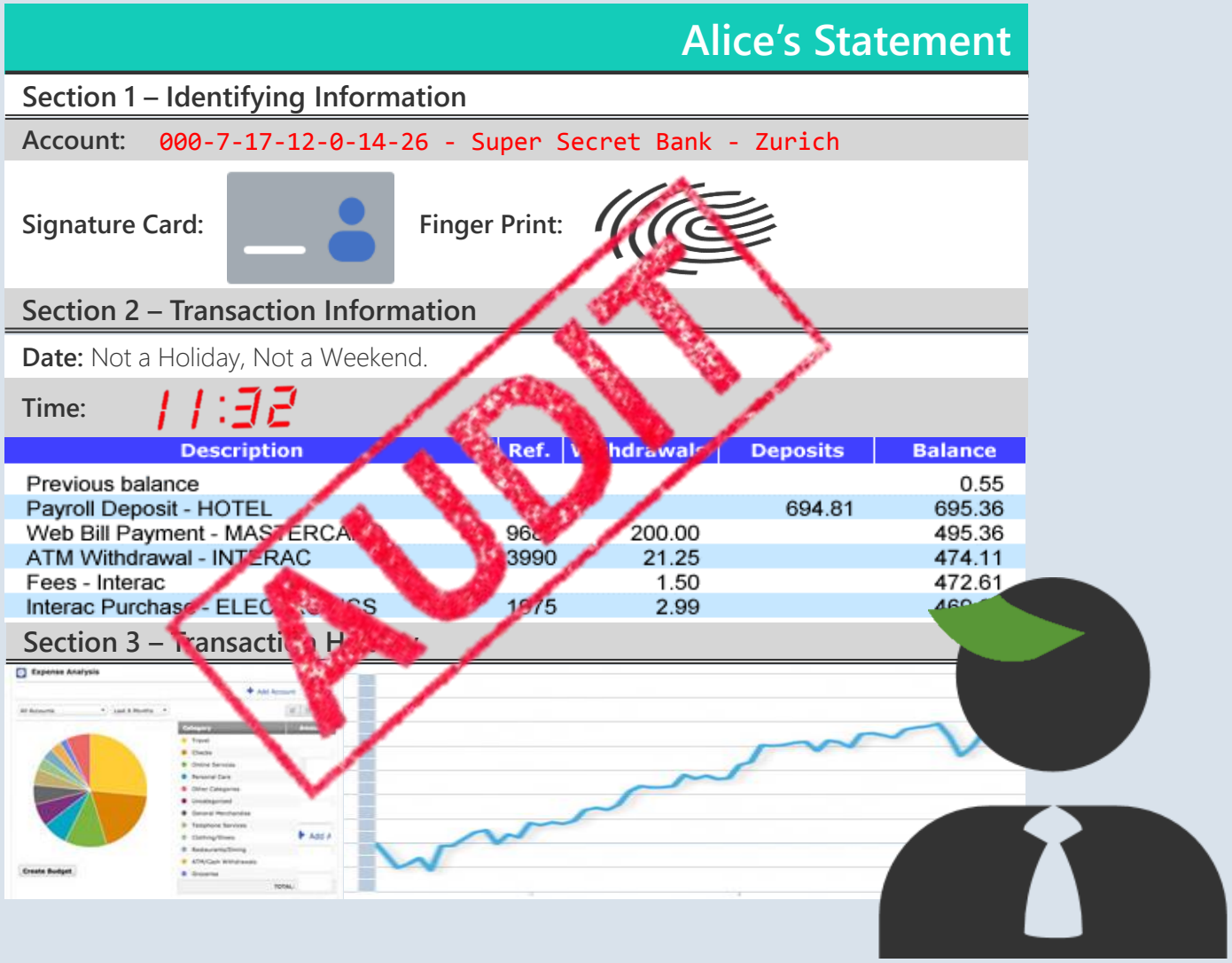
- **Recreate a system state, and events over time, for post facto identification of problems**

Physical World – Bank Statement

- Identifying Information
- Transaction Information
- Transaction History

Digital World

- Account/User Information
- Transaction Information
- Transaction History



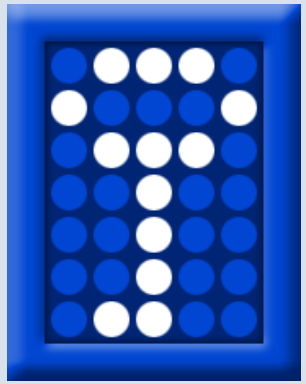
ShieldMyfiles

Applying the Framework

PGP®

1. ✓ Obfuscation
   - Uses Derived Key Cryptography
2. ~ Access Controls
   - Public/Private Key
3. ✗ Auditability

- Separation of Duties



TRUECRYPT

1. ✓ Obfuscation
   - Uses Derived Key Cryptography
2. ~ Access Controls
   - Passphrase/Key Files
3. ✗ Auditability

- Separation of Duties

ShieldMyfiles Applying the Framework Cloud

Google Drive

1. ~~Obfuscation~~
   - Yes, but not from Google
2. ✓ Access Controls
   - Passphrase, Multifactor, Share
3. ✓ Auditability
   - Work Edition

- Separation of Duties

ShareFile by CITRIX

1. ~~Obfuscation~~
   - AES256/TLS256
2. ✓ Access Controls
   - Passphrase, Plugins, Sharing
3. ✓ Auditability
   - Very Nice Dashboards

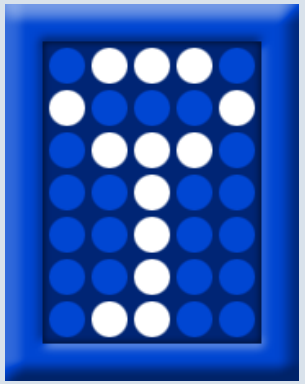
- Separation of Duties

ShieldMyfiles

Meeting the Framework

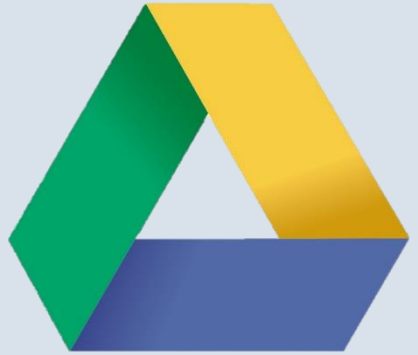
1. Obfuscation
   - Deriving/Issuing keys can be dangerous especially with cloud services
2. Access Controls
   - Need multiple avenues for authorization to fit security to need
3. Auditability
   - Chain of custody is essential

- Separation of Duties
  - Only works if keys are not derived/issued by the Obfuscation, Access Control and Auditability provider
  - Protection WITHOUT Possession



TRUECRYPT

+



Google Drive

ShieldMyfiles

Contact Us

Joseph Webster, CISSP
joe@shieldmyfiles.com
Joseph.Webster@ieee.org

J. Max Romanik, J.D., M.B.A.
max@shieldmyfiles.com

Christopher S. Webster, J.D.
chris@shieldmyfiles.com

Learn More

https://www.shieldmyfiles.com/