YOUR DIGITAL FILE

Technical Overview

Your Presenter

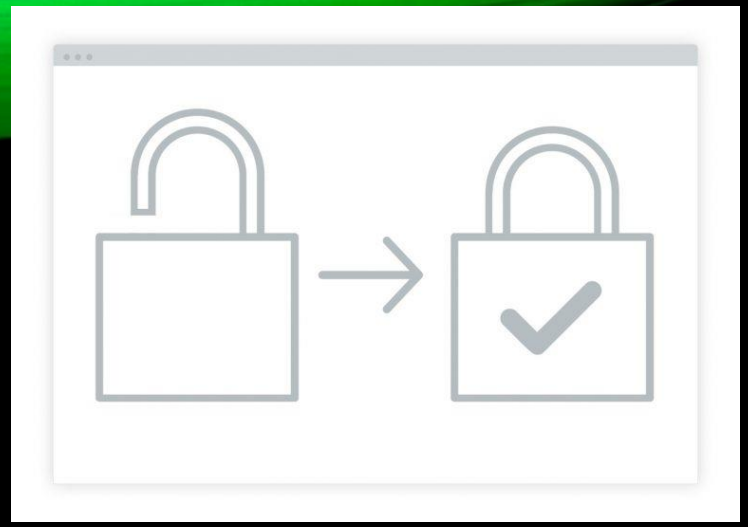
Mark McPherson

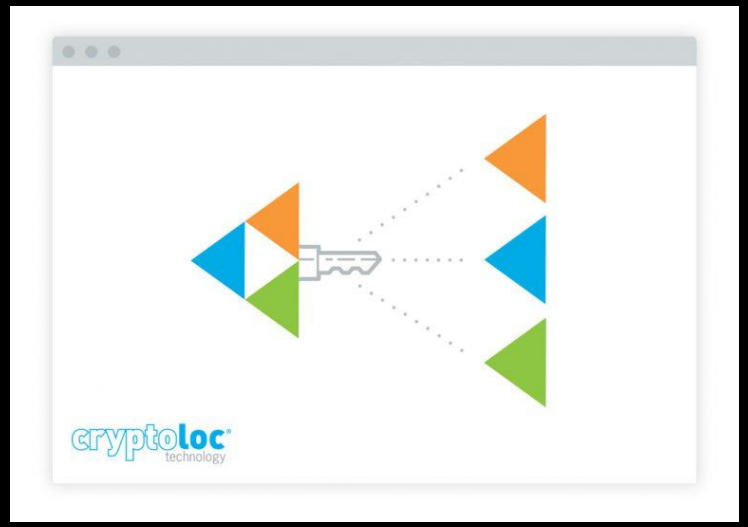
Chief Information Security Officer
Your Digital File

AGENDA

- About Your Digital File (YDF)
- Businesses uses of YDF
- Personal uses of YDF
- How YDF's crypto works
- Attributes of the YDF solution
- YDF architecture – key security and lost keys
  - Solving the key management problem
  - How the escrow works
- Secure File-sharing
- Additional YDF safety and security
- Exceptional uses for YDF (classified storage?)

ABOUT YOUR DIGITAL FILE (YDF)



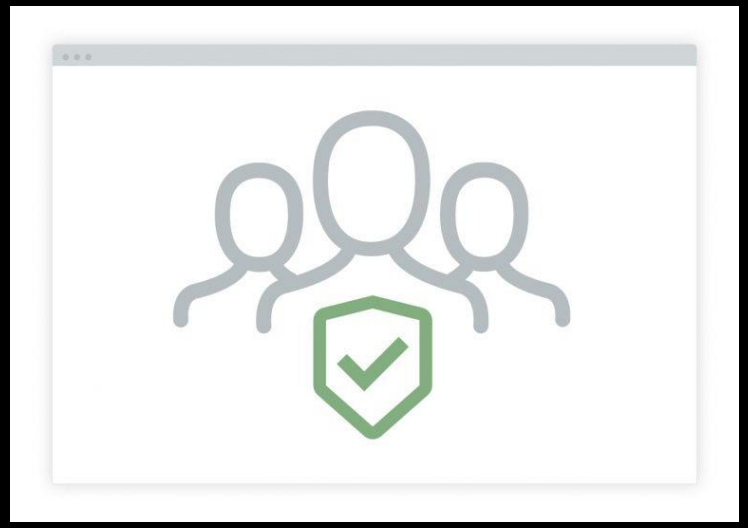


Windows

OS

ANDROID

iOS



YDF *WAS* DESIGNED FOR ***DIGITAL LEGACY***

- To securely store (encrypted) legacy data for an individual (data Owner)
  - Data Owners are **ID verified** (*Green ID service*)
- Encryption keys managed via 3-way share (Owner, YDF & Escrow)
  - aka ***key-splits***
- System allows Owner to grant secure access permission to other individuals
- A **Legacy Event** triggers YDF sharing of data to nominated individual ('next of kin' or legal rep (the *new data owner(s)*)

WHY BUSINESSES MIGHT WANT YOUR DIGITAL FILE

FEATURES **BUSINESSES** MIGHT NEED…

- Data security on the cloud
  - ***SAAS for cloud storage*** (C.I.A. & Industry best-practice encryption)
  - Ease of use (client-proof key management)
  - Peace of mind (zero-touch – **YDF is hands-off**)

- Fraud or data loss protection
  - Ransomware
  - Catastrophic events (fire, flood, malware, malicious damage etc)

- File audit and version control
  - Non-repudiation
  - Recovery of previous file versions

- Digital signing (signatories validated by proof of identity)
  - Green ID – AUSTRAC AML/CTF requirements met

- Secure file sharing

WHY INDIVIDUALS MIGHT WANT YOUR DIGITAL FILE

FEATURES **INDIVIDUALS** MIGHT NEED…

- Data security on the cloud
  - ***SAAS for cloud storage*** (C.I.A.)
  - Ease of use (client-proof key management)
  - Peace of mind (zero-touch – **YDF is hands-off**)
  - Data Legacy (e.g. estate documents) pre-nominated recipients when **events** occur

- Fraud or data loss protection
  - Ransomware
  - Catastrophic events (fire, flood, malware, malicious damage etc)
  - Access to files from anywhere (ID validation and key recovery available)

- File version control and recovery
  - Non-repudiation
  - Recovery of previous file versions

- Secure file sharing
  - Safe method of sharing sensitive files
  - Control in the hands of the individual

HOW DOES YOUR DIGITAL FILE'S CRYPTO WORK?

HOW YDF'S CRYPTO WORKS…(1)

SETUP:

- Client creates a **private/public key pair** (4096-bit RSA) + **password** for account access.

  - **Private key** stored on client device
    - Used for decryption and digital-signing

  - **Public key** is stored by YDF
    - Used during the encryption process and to verify digital signatures

ATTRIBUTES OF THE **YDF SOLUTION**

- Encryption mechanism protects the **confidentiality, integrity & privacy** of your sensitive documents on the cloud

- Audit mechanism means that:
  - you will always know ***when*** a file on the cloud was ***uploaded*** or ***modified***

  and
  - When sharing files on the cloud with non-YDF users:
    - know when a file is downloaded
    - grant or revoke access manually or after a specific time period.
    - provide a **secure upload** area for a non-YDF user or users
      (contents cannot be viewed or modified)

YDF TECHNOLOGY

Zero Trust Encyption

You have a personal "key" – accessible only by you. Data is encrypted for the client before it reaches YDF. This means that unlike other institutions we do not access your data in any way.

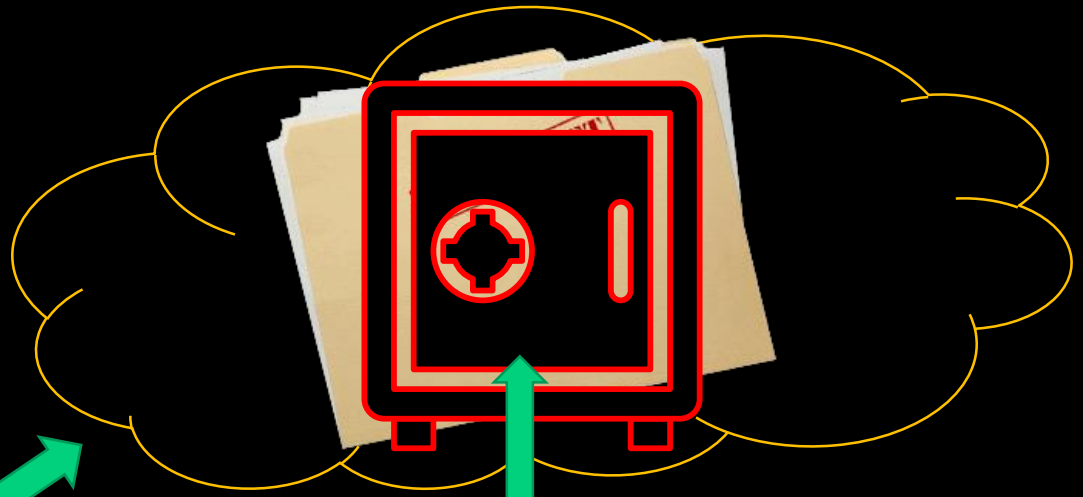
Unbreakable Administration

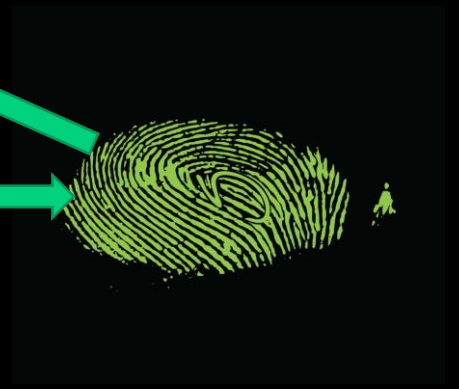
Your personal key is made up of three independent parts which create the layer of security to protect you from theft or fraud. However, recovery keys are accessible by the account holder in the event of one of life's unexpected events.

Cryptographic Forest

Each file version is encrypted with a separate random key. Each authorised relationship for that file generates another key. This means that if a hacker could break the encryption on a file, they would only get access to that file and no others. The file is a tree, each key is a branch, branching again when a new user is granted access. Breaking the branch at that point may compromise the tree at that point but it does not compromise the forest.

HOW DOES YDF STORE FILES?





HOW YDF'S CRYPTO WORKS…(2)

FILE UPLOAD:

- The YDF software generates **3 symmetric keys** (random AES-256) on the client (aka the ***key-splits***)
  - Collectively, they form the Document Encryption Key (DEK)
  - The **DEK** is used to encrypt the file prior to upload to the cloud
    - The client device **duplicates each key-split** and groups them in **pairs** of different splits.
    - These **key-split pairs** are then individually encrypted using the public-keys of each the 3 different parties in the YDF "Shared Secret" key management mechanism ***(more on this in a minute…)***
  - The **encrypted file** and the **encrypted key-split pairs** are then stored separately on the cloud by the YDF system for later retrieval

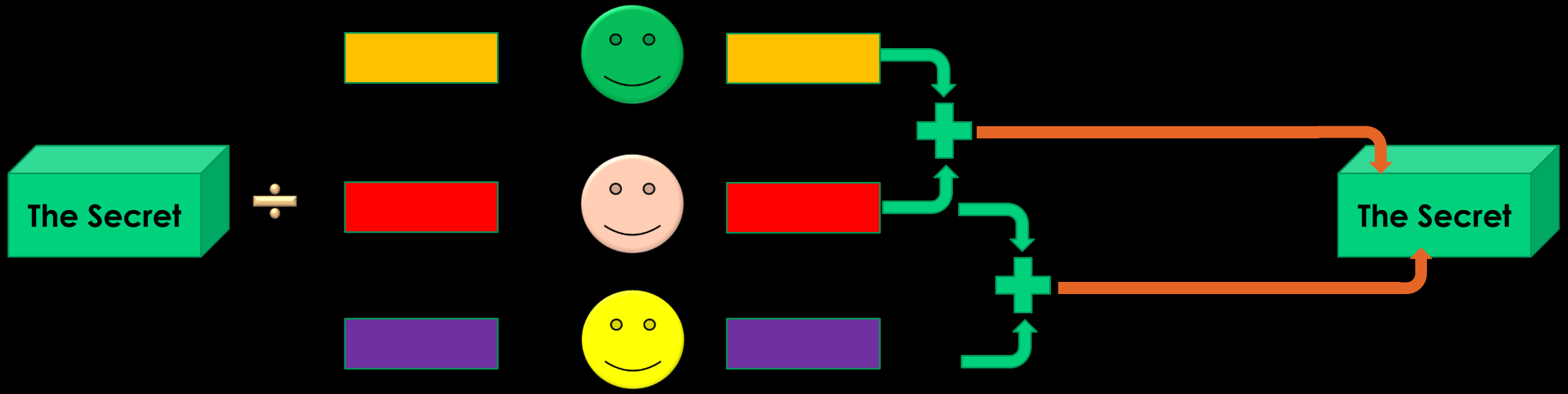
NOTE: Signatures and fingerprints are calculated and recorded at various steps along the way to check and ensure file integrity during transmission over the network and to be used for non-repudiation

YDF ARCHITECTURE – KEY SECURITY AND LOST KEYS

SOLVING THE KEY MANAGEMENT PROBLEM

- Shamir's Secret Sharing mechanism
- YDF's implementation of SSS
- Role of the Escrow

SHAMIR'S SECRET SHARING – *SIMPLE EXAMPLE*



"The secret (i.e. the cryptographic key) is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret."

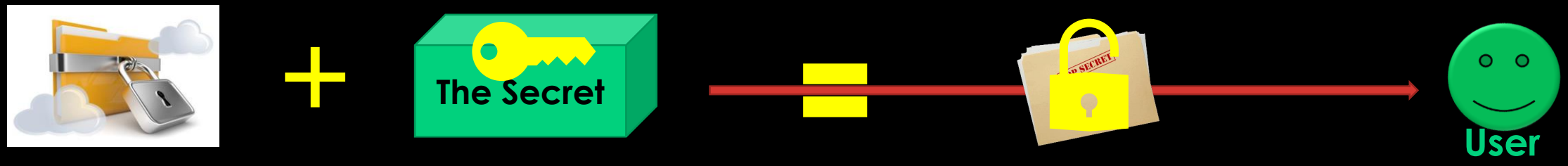
Ref: http://cryptography.wikia.com/wiki/Shamir%27s_Secret_Sharing

HOW ARE SECRETS USED?

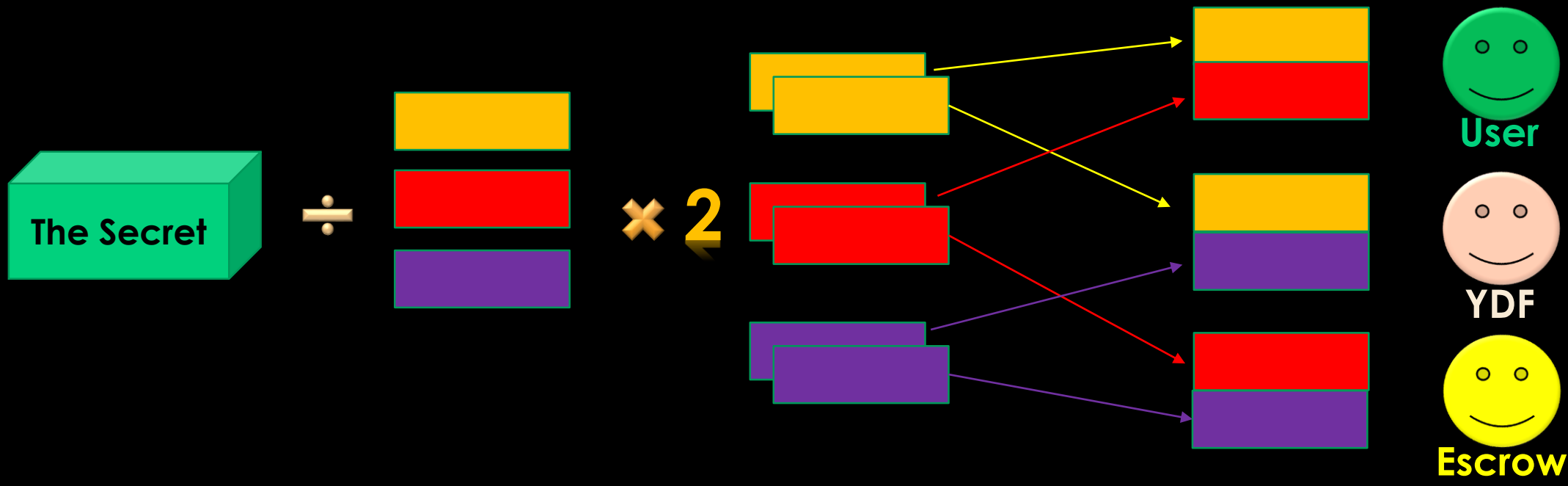
FILE UPLOAD AND DOWNLOAD

FILE UPLOAD:

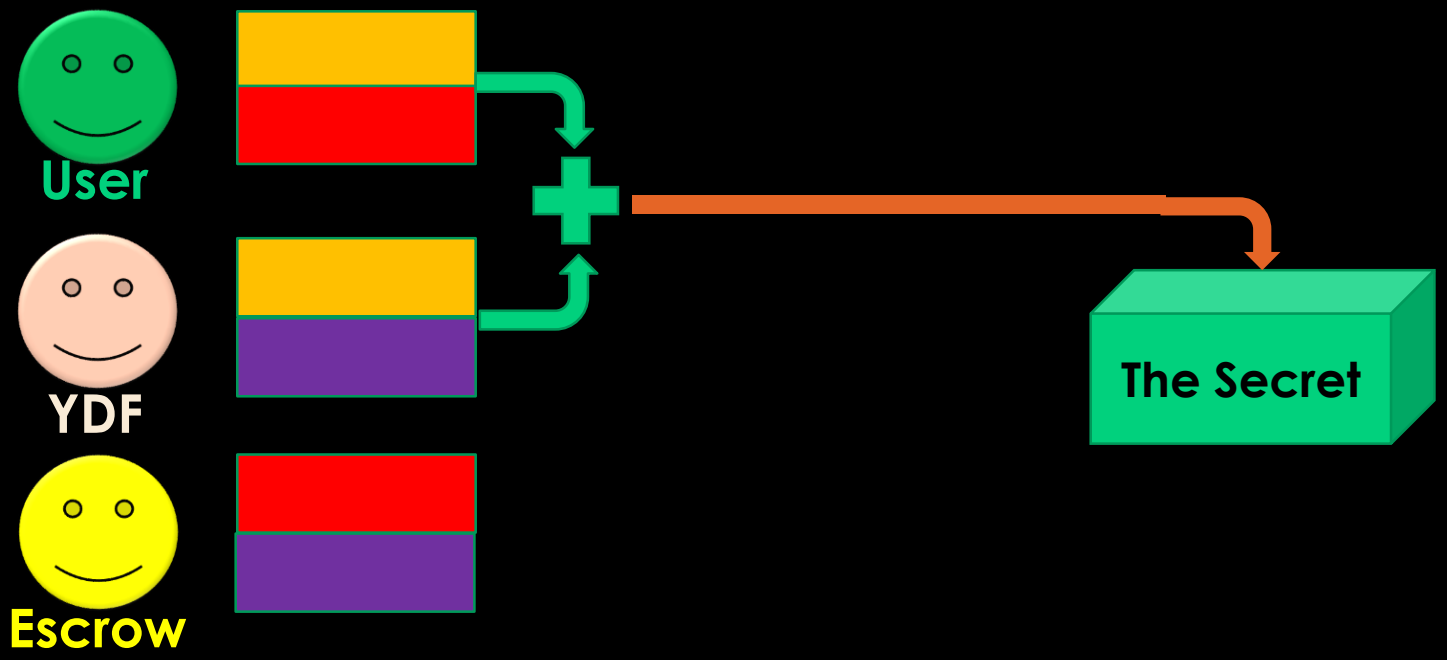
FILE DOWNLOAD:



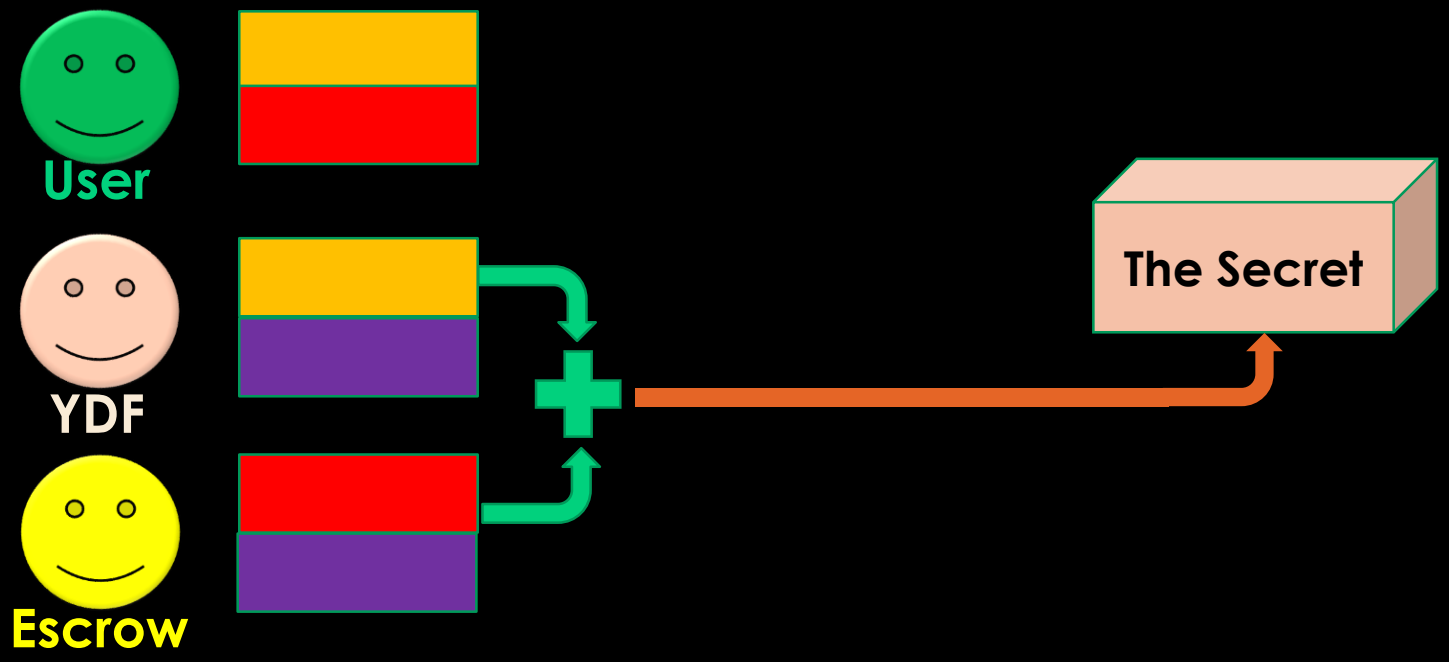
SHAMIR'S SECRET SHARING – *YDF-STYLE*



ACCESS TO FILES ***VIA YDF*** DURING B.A.U.



ESCROW'S ROLE IN ***KEY 'RECOVERY'***



ESCROW'S ROLE IN ENSURING CONFIDENTIALITY

- The YDF **Escrow Agent** is a separate legal entity to YDF (in our case a legal firm)

- If a YDF client requests **key recovery**, the Escrow agent must agree first that the request is legitimate and can (if desired) undertake additional due diligence such as requiring an ID check or requesting documents from a business client to support their access claim

- Your Digital File Pty Ltd must also agree that the request is legitimate

Unless both parties agree, 'recovery' cannot continue!

- Once the parties agree, the Escrow agent accesses the YDF system with a special private key that grants them the ability to initiate the escrow process
  - The client is invited to generate a new private key and password
  - Depending on the number of files stored, the process of 'key recovery' can take some time; as all key-splits must be re-encrypted and stored for each file

HOW YDF'S CRYPTO WORKS…(3)

FILE ACCESS/DOWNLOAD:

- To **download a file**, the file owner* requests access to that file from YDF
  (who authenticates themselves to the YDF system via their username and password and the presence of their private key)*

- The YDF system grants the file owner access to an **unencrypted version of YDF's pair of key-splits** for that file and the owner decrypts **their own pair of key-splits** with their private key.

- Because two parties can provide the key-splits needed to form the **full DEK**, the file owner can decrypt the file on download.

YDF SECURE FILE-SHARING

FILE ACCESS GRANTS TO OTHER YDF USERS:

- To grant access to a encrypted file stored via YDF, the **file owner** identifies the recipient (either via their YDF login ID and instructs the YDF system to grant them access.
- The YDF system then grants the recipient access to the **current version** of the file by encrypting a part of the DEK (i.e. the key-split owned by the YDF system) with the public key of the recipient; allowing them to join the list of users authorised to access the file; but this does not transfer full ownership of that file to the recipient.

- The recipient of a shared file can decrypt the file on download using their private key.

YDF SECURE FILE-SHARING (2)

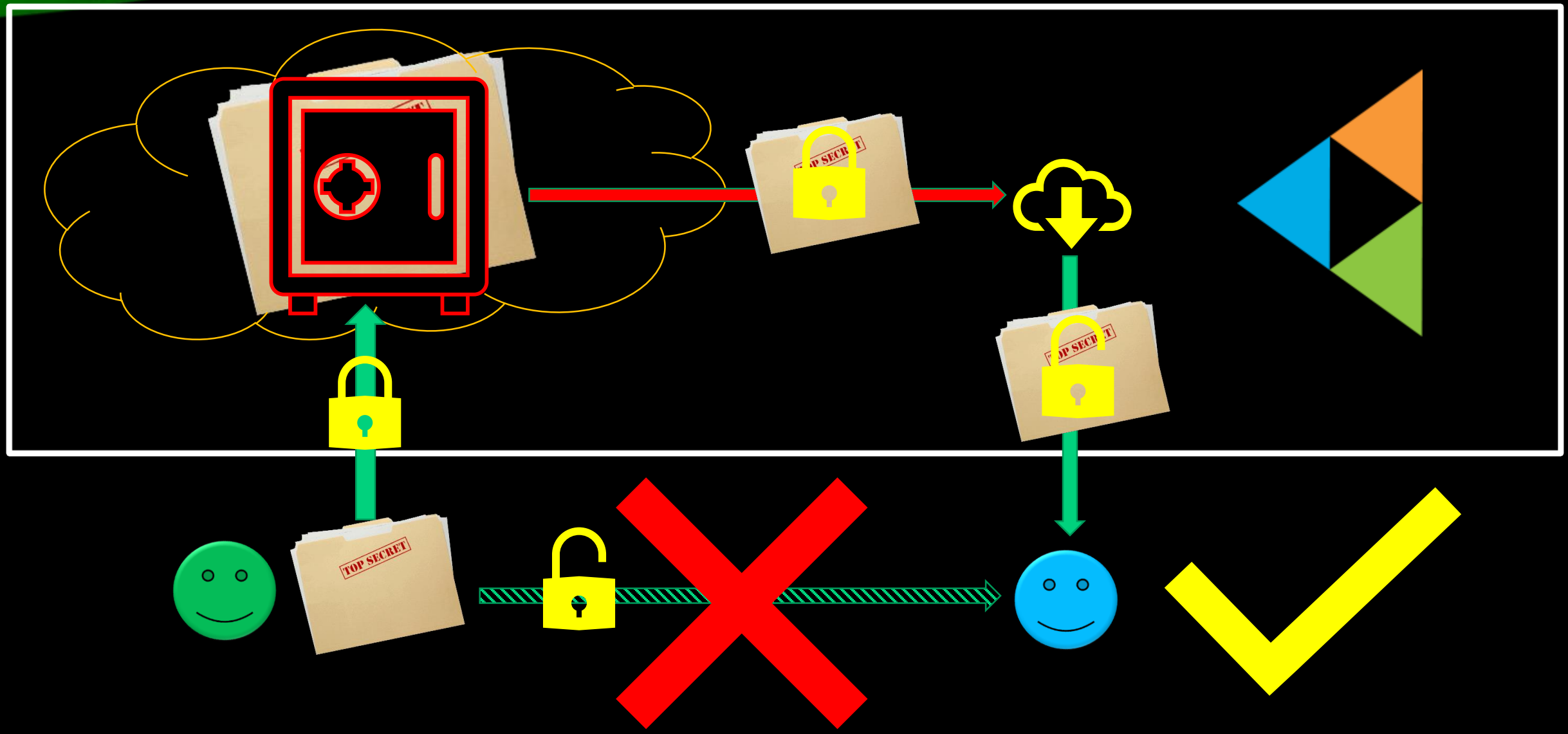
FILE ACCESS GRANTS TO NON-YDF RECIPIENTS OF A YDF "SecureShare":

- A YDF-user identifies an **non-user** via their email address and Mobile phone number.
- The system is instructed to send an email to the recipient.
- If the recipient is a **non-YDF user**, a new randomly-keyed encrypted version of the file is created with a one-time decryption key sent once the recipient has entered a one-time SMS code as a response to the email message they received.
- This tells the YDF system to download the file to the recipient's device and decrypt it locally.

FOR BOTH TYPES OF YDF FILE-SHARING:

- Activities such as downloads are logged by the YDF audit mechanism
- Digitally-signed documents are hashed and timestamped
- Confirmation or access options (e.g. 'update', 'sign as received' or 'sign and agree') can be selected by a YDF-user making a file-share to someone

SECURE FILE SHARING…



ADDITIONAL YDF SAFETY AND SECURITY

- All network communications between client devices and YDF servers use **TLS tunnels**
- All **encryption** is performed **client-side**; no files pass over the network unencrypted
- Updates to stored files always create **new versions** & all **activity is logged**
- Secure-share: external parties receive **one-time encrypted copies** of the **current version** of a file
- YDF uses highly-resilient **AWS cloud services** including:
  - Logical isolation of YDF web application
  - Client data hosted in Australia (Sydney) with VPCs spanning multiple Availability Zones (Sydney and Melbourne)
  - YDF uses 'Cloudfront" (CDN) as a first-layer of *WAF*

EXCEPTIONAL USES FOR YDF

CLASSIFIED STORAGE?

- YDF provides a platform that integrates:
  - The secure (encrypted) storage of files
  - A verification system for user identities
  - Group and individual file permission structures
  - An access revocation mechanism
  - File-based audit
  - Automated one-way update file versioning
  - Escrow oversight of user key management

- Classified documents ***could*** be stored and shared within a YDF organisational account (aka 'Business account') **so long as** the cloud storage and the end user devices were certified to the required level/to the satisfaction of the client
- YDF's cloud storage and organisational processes are not **currently** cleared for classified storage

QUESTIONS?

https://www.yourdigitalfile.com