SMU
SINGAPORE MANAGEMENT UNIVERSITY

School of
Computing and
Information Systems

Achieving Cloud Data Security and Privacy in Zero Trust Environment

-- From cryptographic research to system implementation

Robert Deng
AXA Chair Professor of Cybersecurity
School of Computing & Information Systems
Singapore Management University

11 August 2022

Agenda

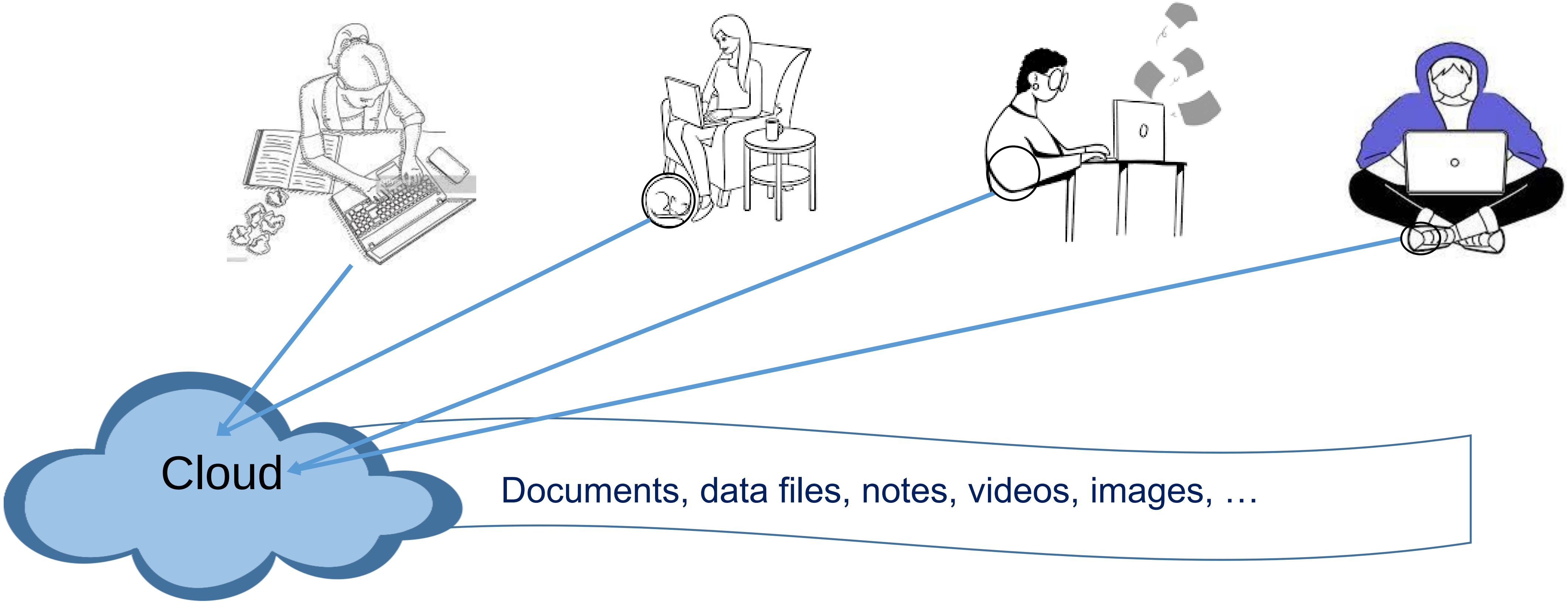
Introduction

sBox – Cloud Data Security & Privacy Platform in Zero Trust Environment

Underlying Cryptographic Techniques

Conclusion

Cloud Data Access and Sharing Anywhere Anytime



Cloud

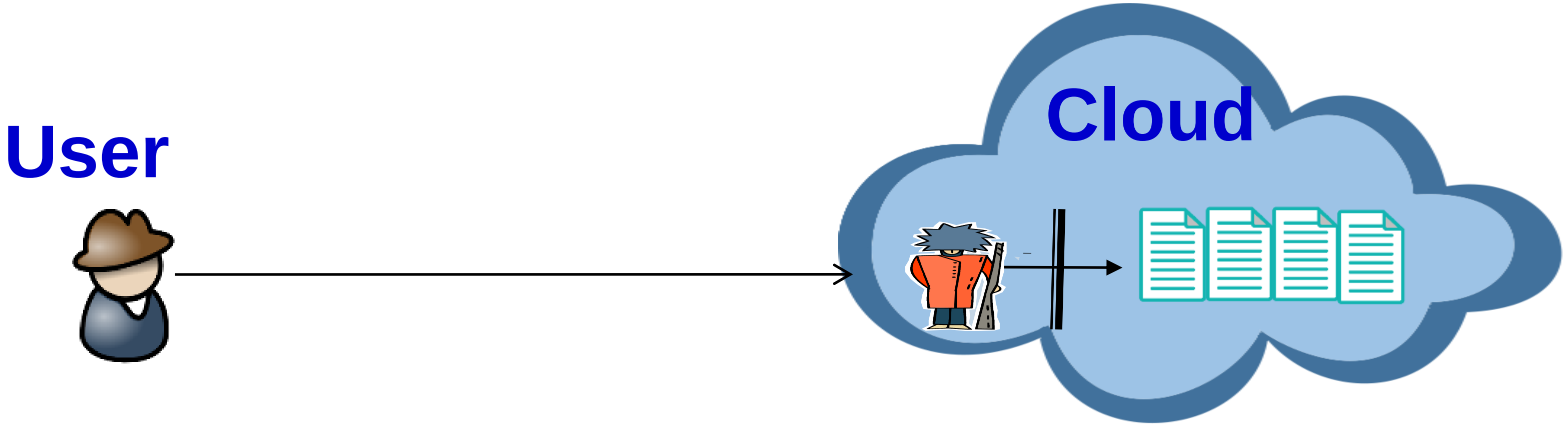
Documents, data files, notes, videos, images, …

Data Breaches Are A Growing Risk

(IBM Cost of a Data Breach Report 2022)

- The report is based on analysis of real-world data breaches experienced by 550 organizations globally between Mar 21 to Mar 22
- 83% of the organizations have experienced more than one breach in their lifetime
- The global average cost of data breaches reached an all-time high of $4.35 million in 2022 compared with $4.24 million in 2021

Root Causes of Data Breaches



- **Compromised credentials, phishing and cloud misconfiguration were the top attack vectors - **IBM Cost of a Data Breach Report 2022
  - Stolen or compromised credentials were responsible for 19% of breaches
  - Phishing was responsible for breaches 16% of the time
  - Cloud misconfiguration caused 15% of breaches
- **“When an online service is free, you’re not the customer. You’re the product”** – Tim Cook

Data Privacy Regulations

- **EU GDPR**
  - EU imposes hefty fine against companies for violation of GDPR (maximum fine of €20 million or 4% of annual global turnover)
- **California Consumer Privacy Act (CCPA)**
  - Imposes stiff penalties for lost records of up to $750 per consumer per incident
- **China Data Security Law**
  - Violations will trigger penalty fines and even suspension of business and revocation of license or permits
  - Person directly in charge of implementing compliance at the company will be exposed to penalty risks

Agenda

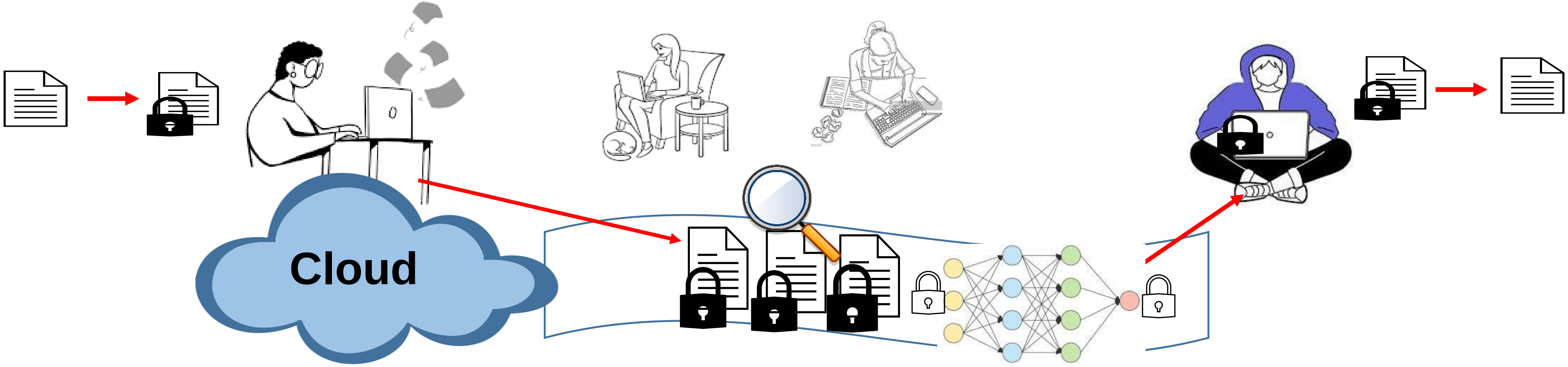
Introduction

sBox – Cloud Data Security & Privacy Platform in Zero Trust Environment

Underlying Cryptographic Techniques

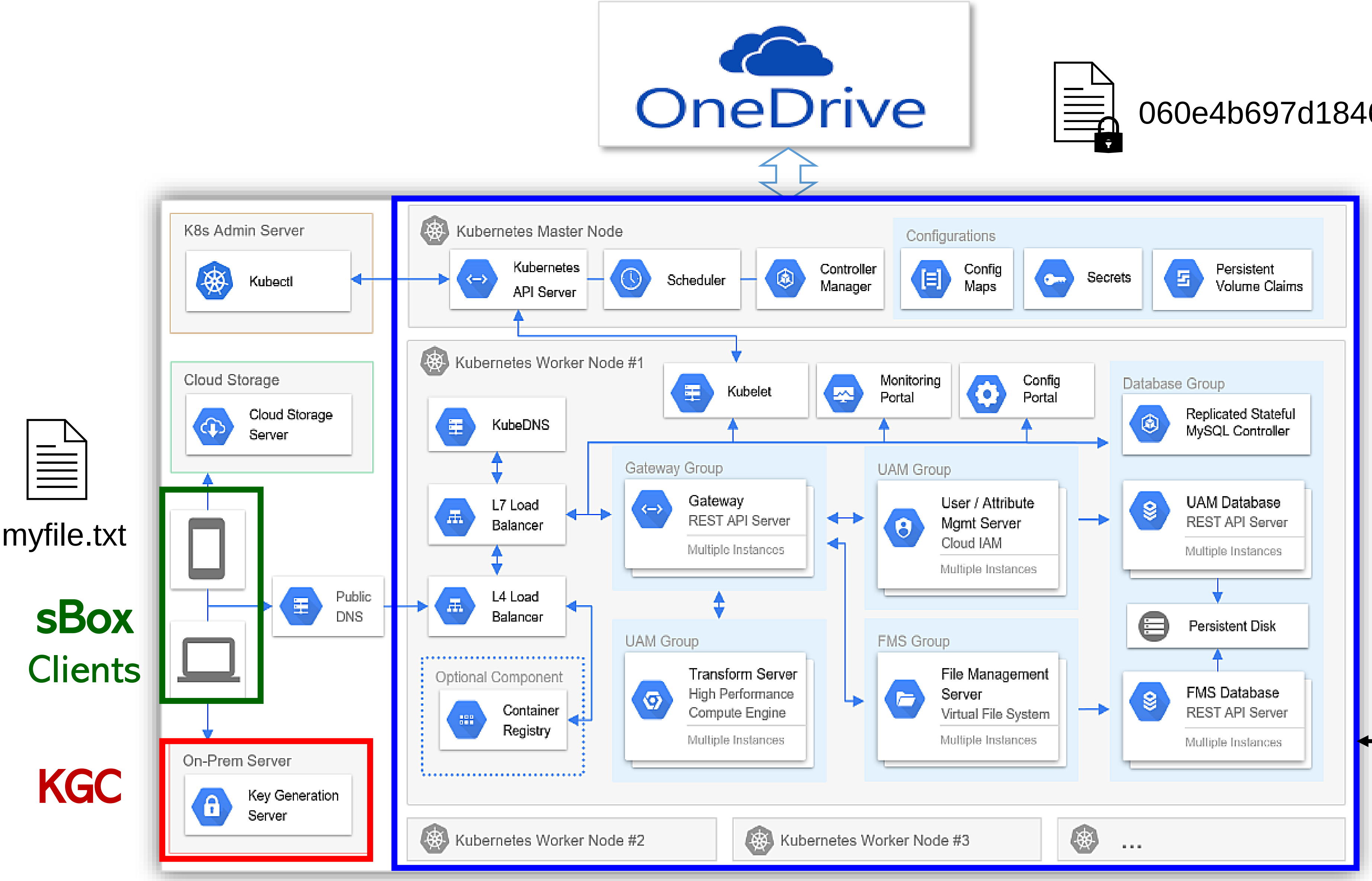
Conclusion

sBox – Cloud Data Security & Privacy Platform in Zero Trust Environment



- **E2E (End-to-End) encryption** protecting data privacy even if user login credentials or the cloud storage is compromised
- **Good usability** – Scalable access control, search, and computation over encrypted data
- **Low operational overhead** - Simple cryptographic key management including efficient user revocation

sBox Architecture & Implementation



myfile.txt

sBox Clients

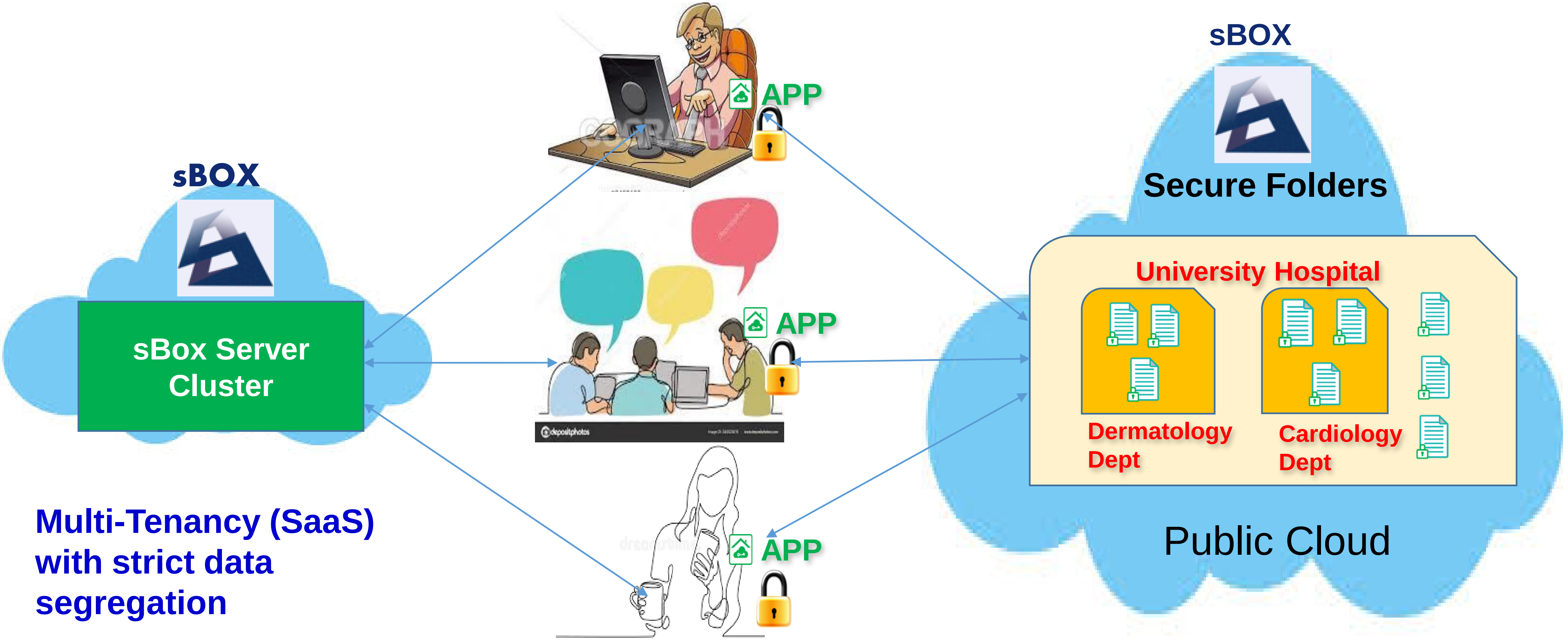
KGC

060e4b697d1846e3a7b

- **Virtual File System**
  - File name→ pseudo name
  - ABE access policy
  - keyword index
  - Folder access permissions
- **Ciphertext transformation**
- **Encrypted keyword search**
- **User revocation**

sBox server cluster

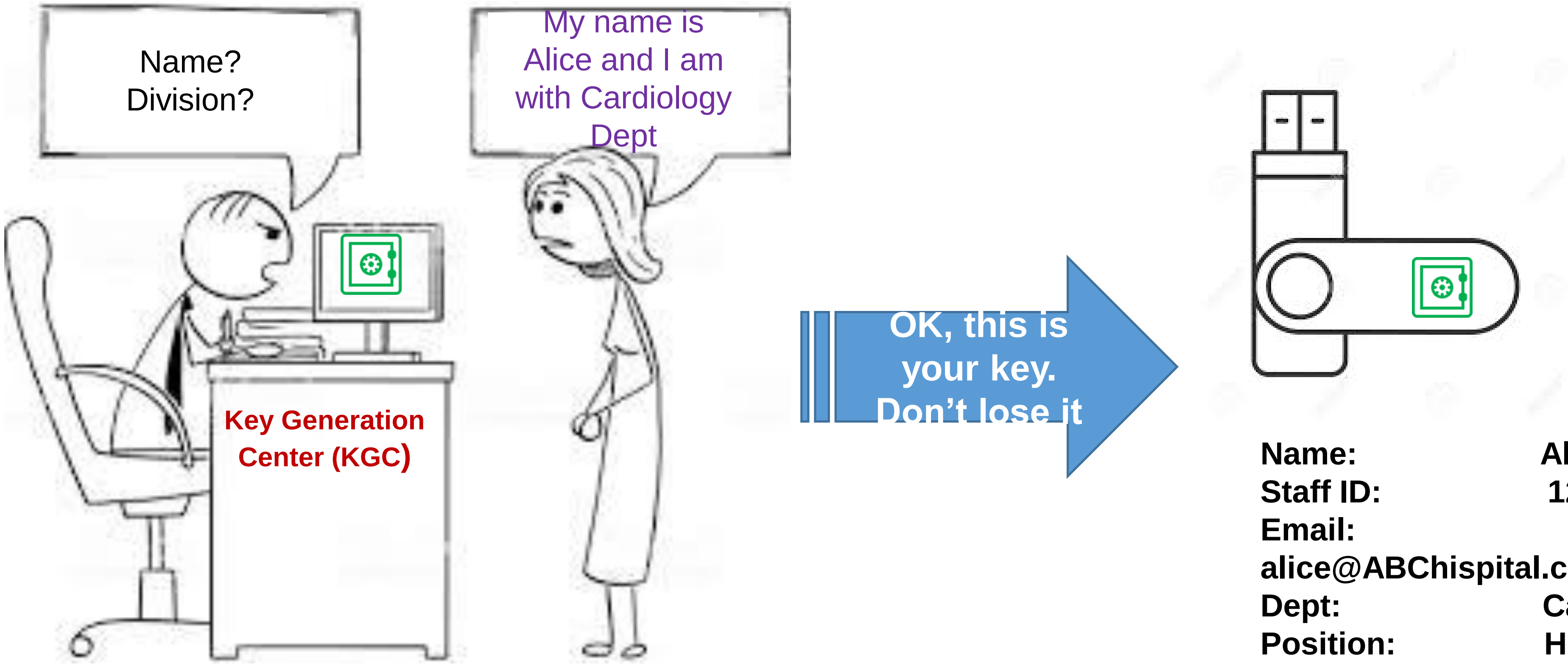
sBOX Deployment Scenarios



Multi-Tenancy (SaaS) with strict data segregation

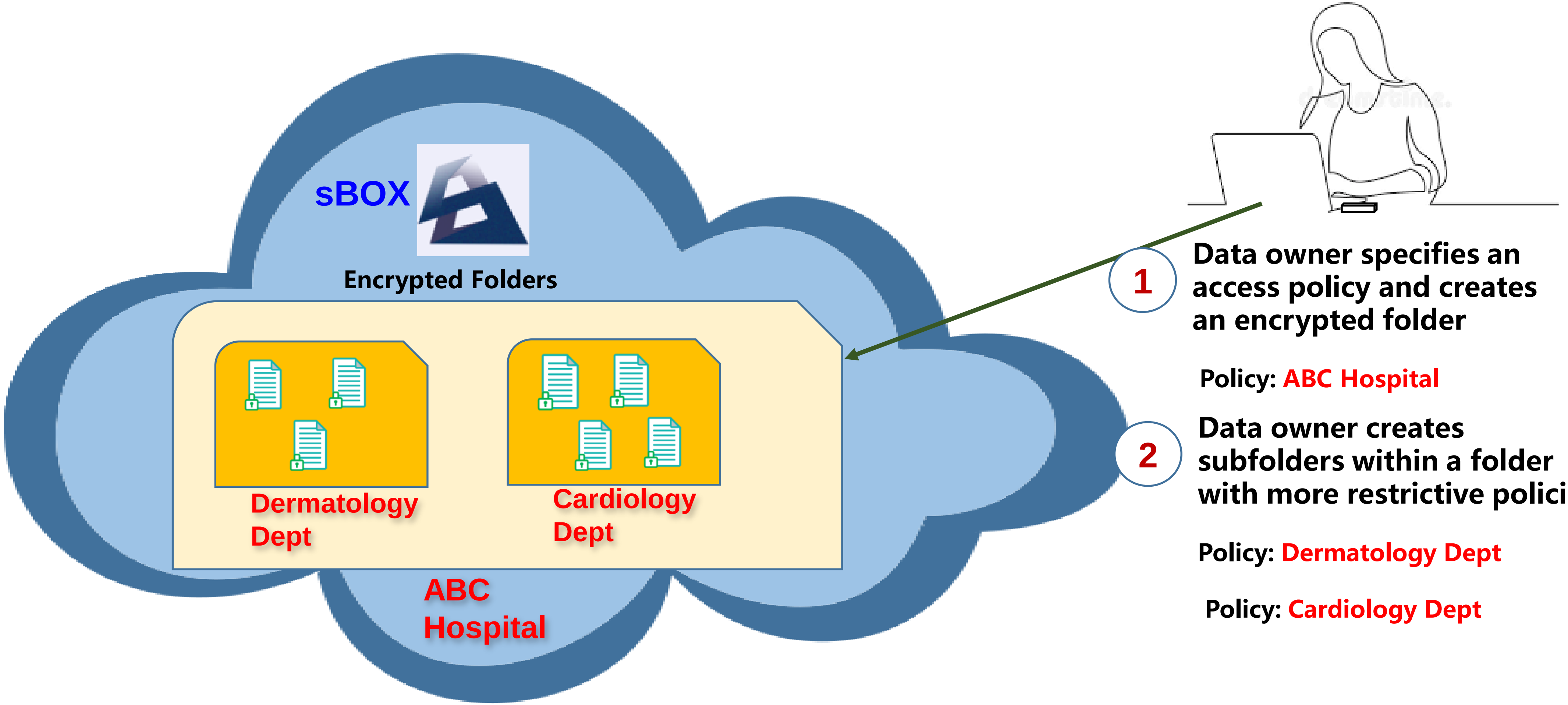
On-Premises

User Enrolment – One Time Process


Name?
Division?
My name is Alice and I am with Cardiology Dept
Key Generation Center (KGC)
OK, this is your key. Don't lose it

Name:	**Alice**
Staff ID:	**123**
Email:	**alice@ABChispital.com**
Dept:	**Cardiology**
Position:	**Head**
Rank:	**Consultant**
Public Parameter:	**XXXXXXXXXXXX**
Private Key:	**YYYYYYYYYYYYY**

Creating Encrypted Folders



Data owner specifies an access policy and creates an encrypted folder

Policy: ABC Hospital

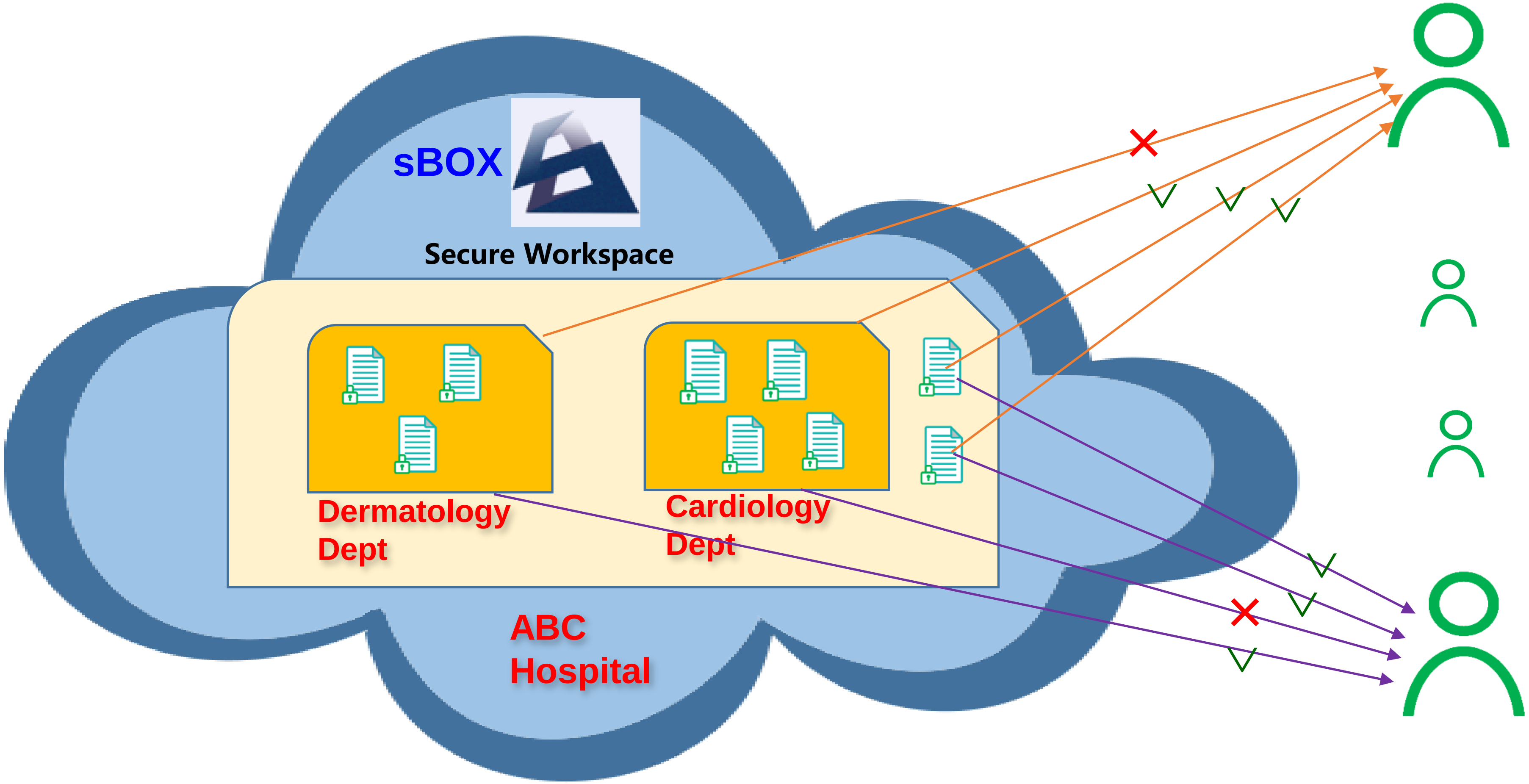
Data owner creates subfolders within a folder with more restrictive policies

Policy: Dermatology Dept

Policy: Cardiology Dept

Double Layers of Access Control

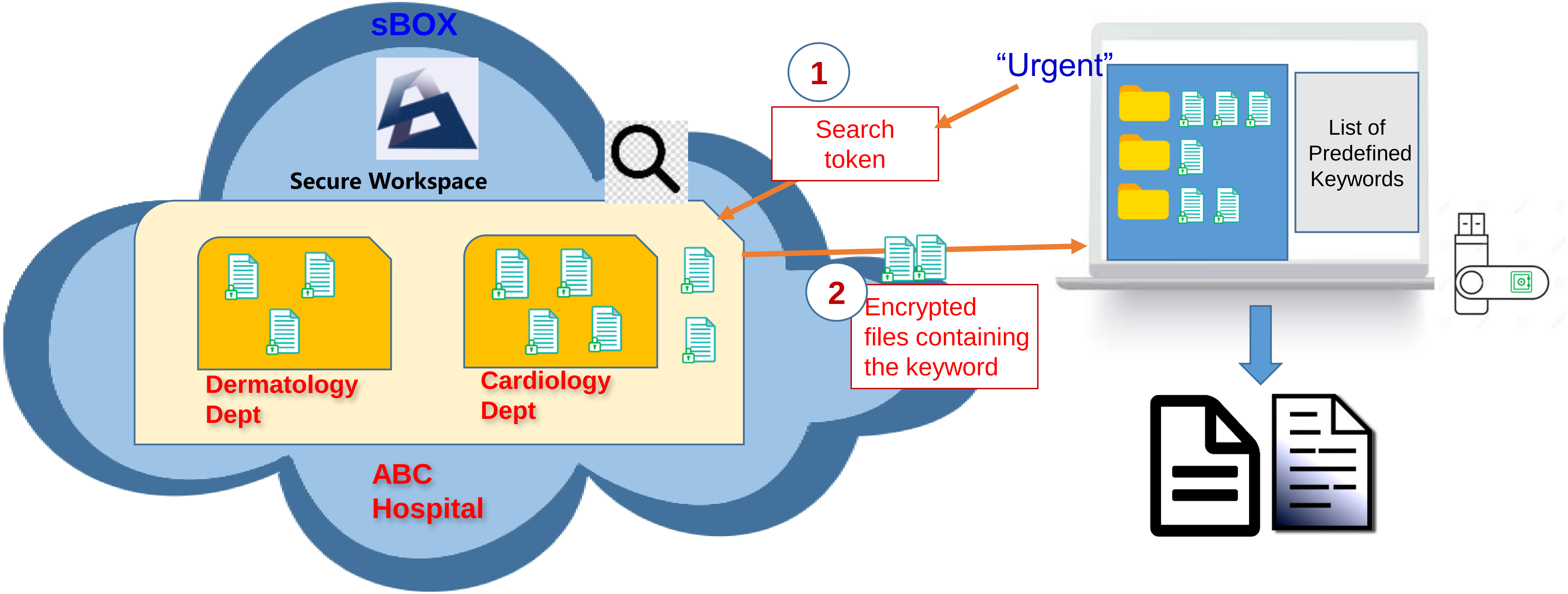
- Access to Folders Controlled by Sbox Server Cluster
- Access to Files Controlled by Crypto



Name:	Alice
Staff ID:	123
Email:	alice@ABChispital.com
Company:	ABC Hospital
Dept:	Cardiology
Position:	Head
Rank:	Consultant
Public Parameters:	XXXXXXXXXXXX
Private Key:	YYYYYYYYYYYYY

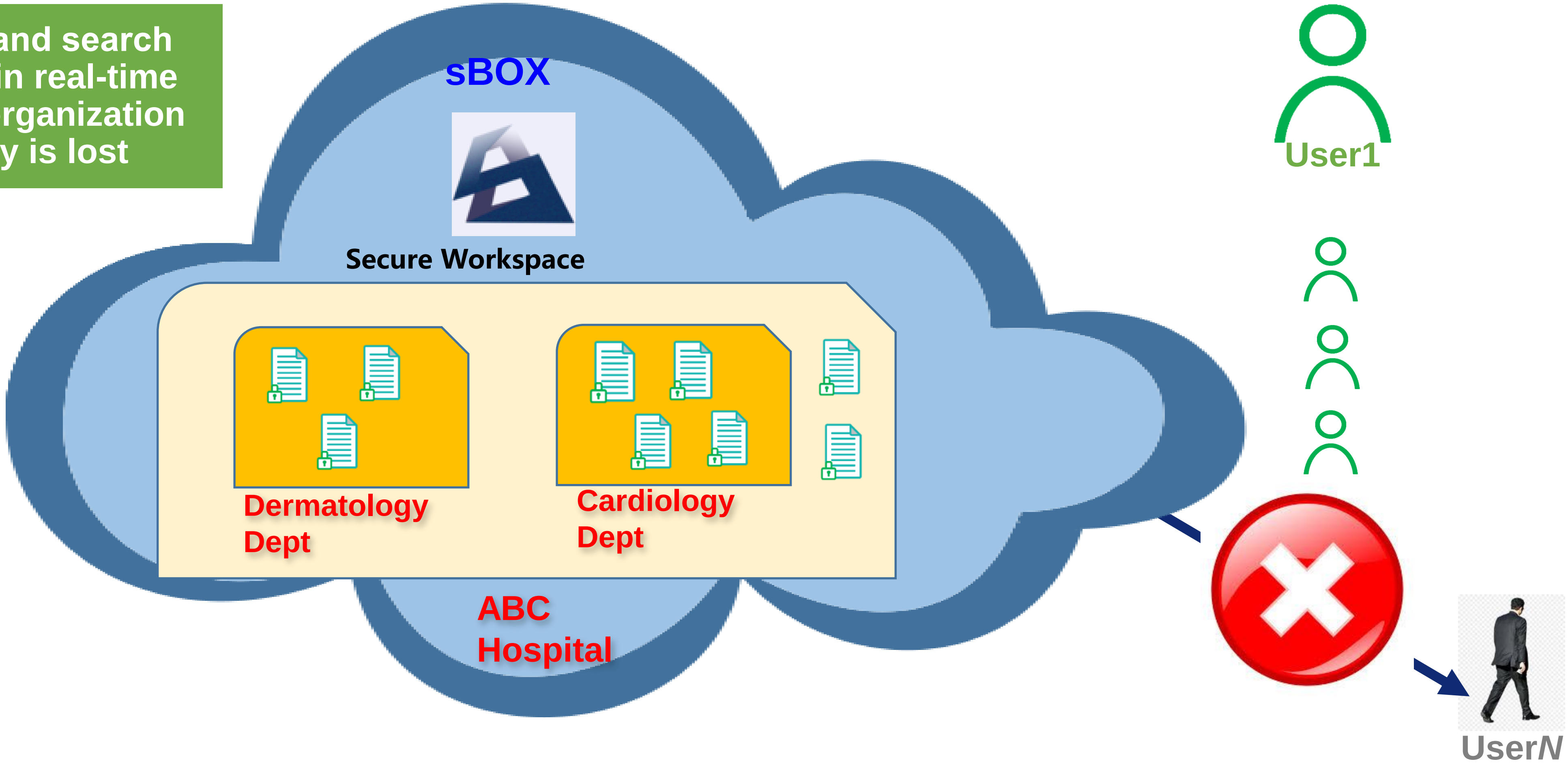
Name:	Bob
Staff ID:	789
Email:	bob@ABChispital.com
Company:	ABC Hospital
Dept:	Dermatology
Position:	NIL
Rank:	Senior Consultant
Public Parameters:	XXXXXXXXXXXX
Private Key:	YYYYYYYYYYYYY

Encrypted Keyword Search



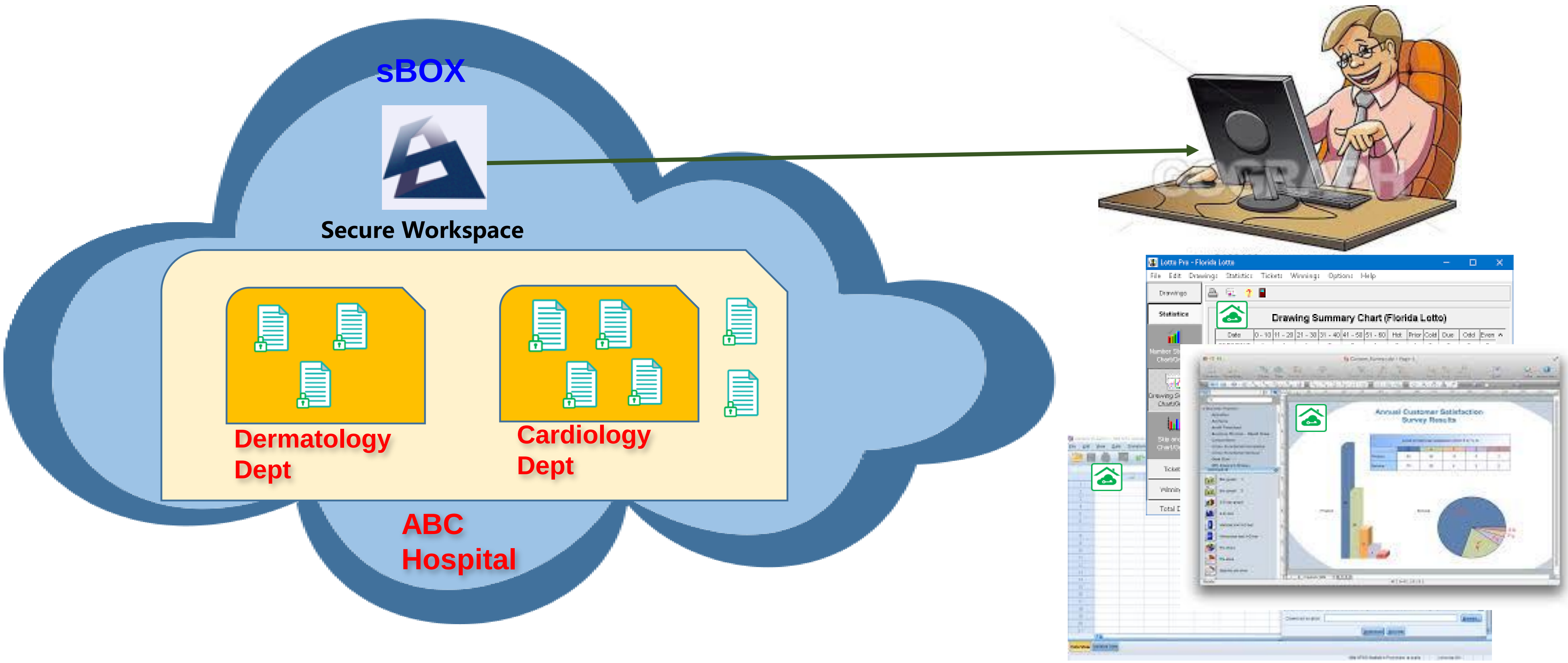
Real-Time User Access Rights Revocation

User's decryption and search rights are revoked in real-time when the user left organization or his private key is lost

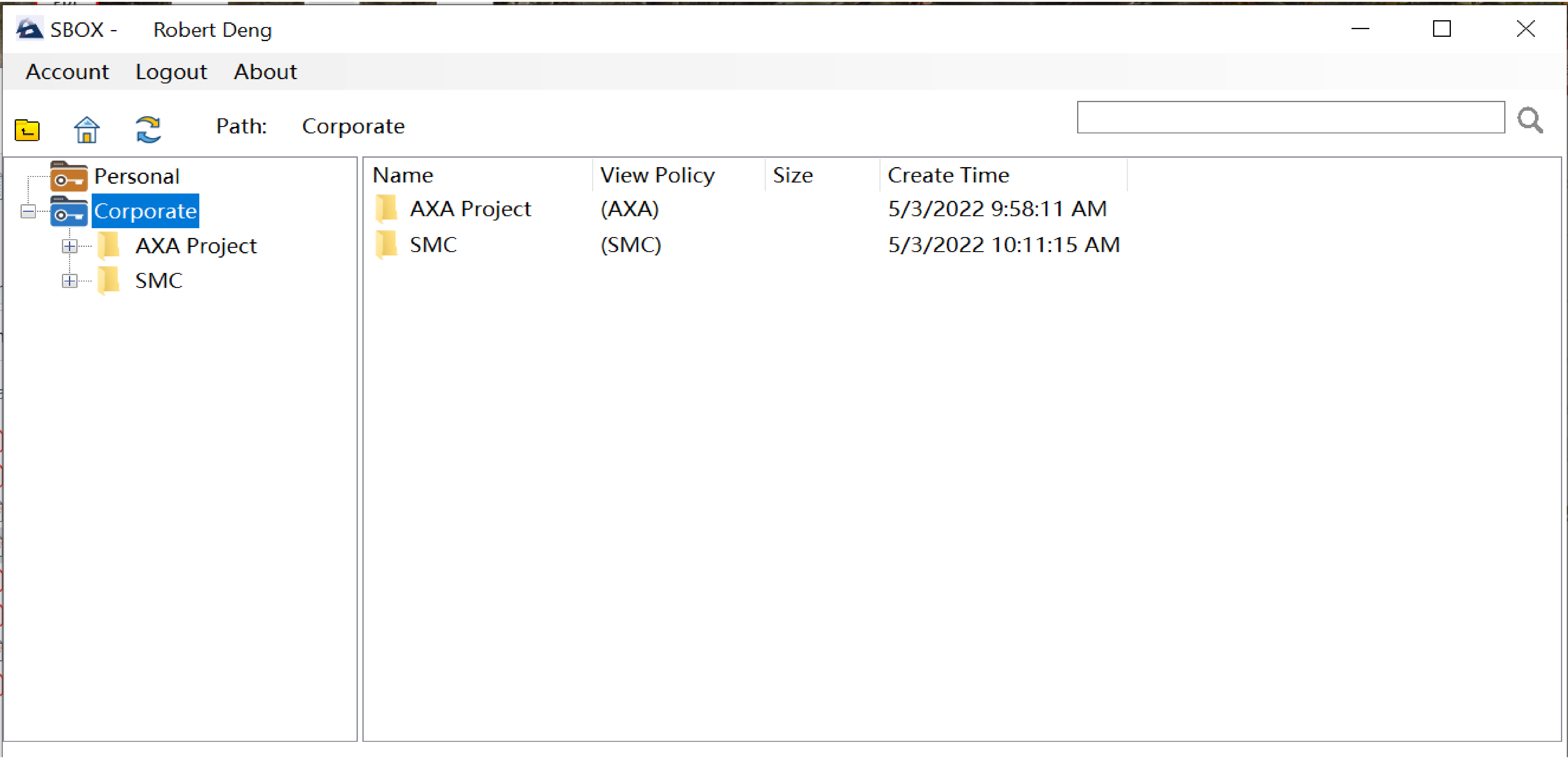


Auditing Log

Customized reporting on activities monitoring & management

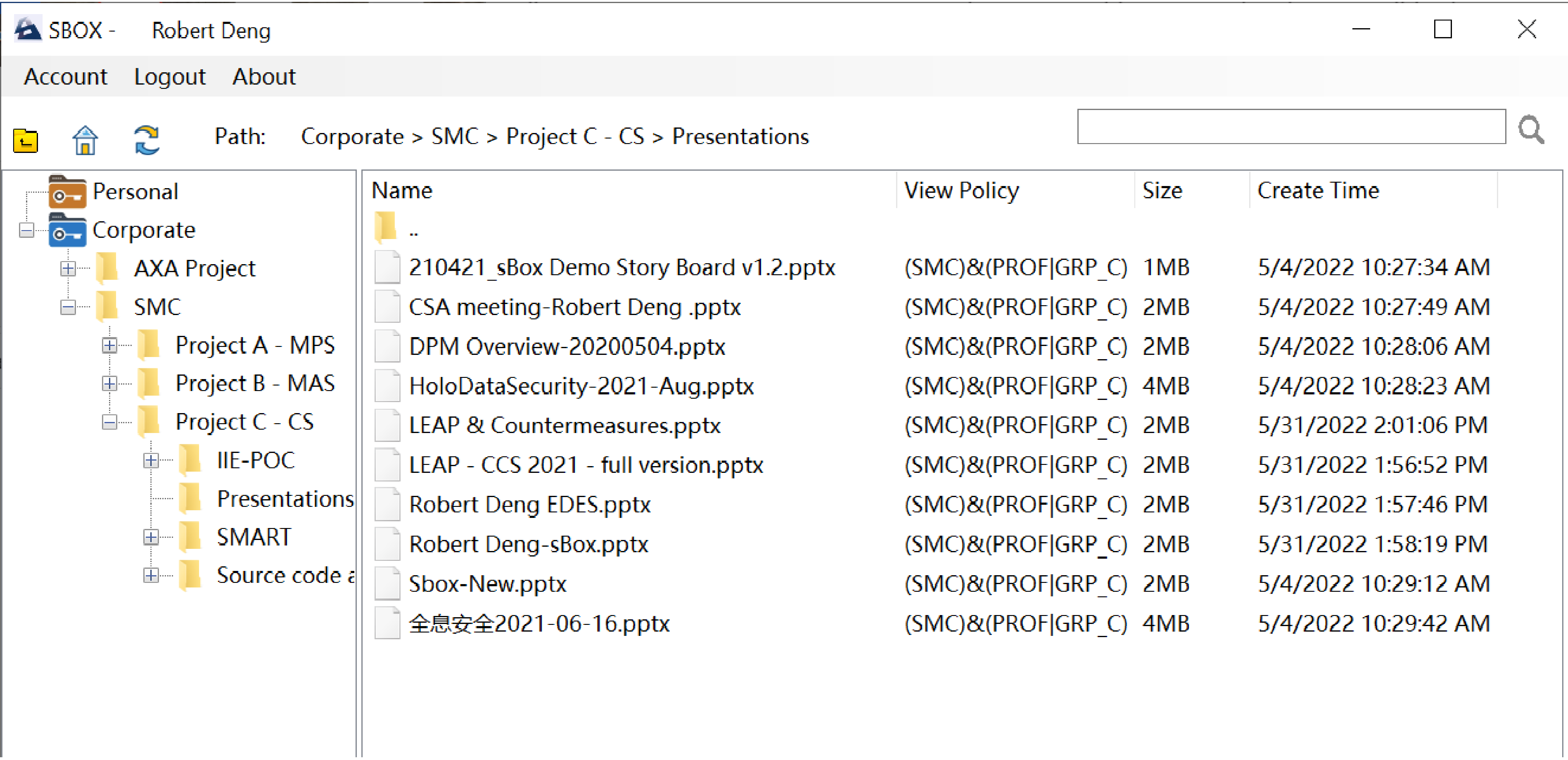

sBOX
Secure Workspace
Dermatology Dept
Cardiology Dept
ABC Hospital
Lotto Pro - Florida Lotto
File Edit Drawings Statistics Tickets Winnings Options Help
Drawing Summary Chart (Florida Lotto)
Annual Customer Satisfaction Survey Results

sBox Screen Shot



Name	View Policy	Size	Create Time
AXA Project	(AXA)		5/3/2022 9:58:11 AM
SMC	(SMC)		5/3/2022 10:11:15 AM

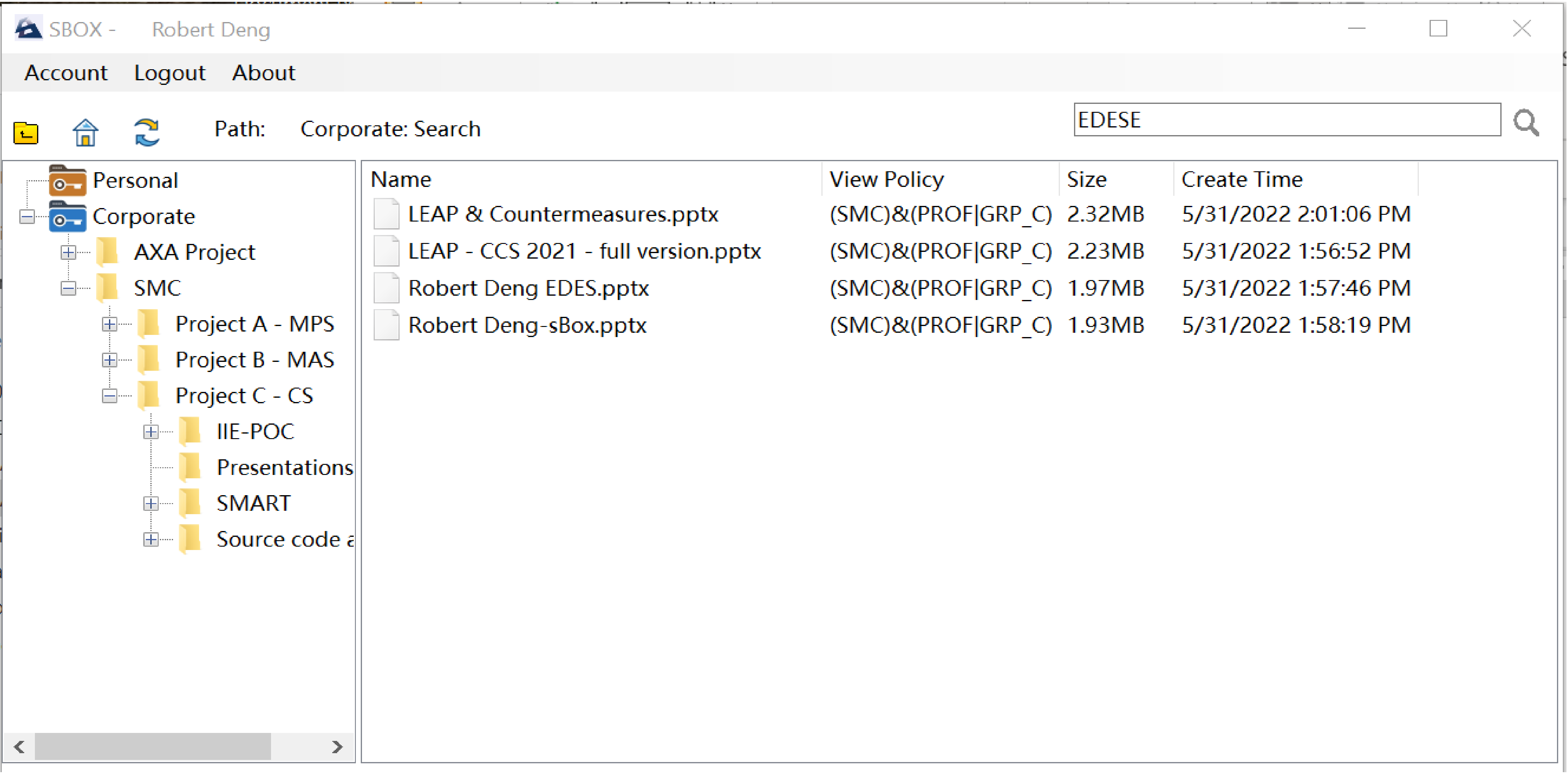
sBox Screen Shot



Path: Corporate > SMC > Project C - CS > Presentations

Name	View Policy	Size	Create Time
..			
210421_sBox Demo Story Board v1.2.pptx	(SMC)&(PROF|GRP_C)	1MB	5/4/2022 10:27:34 AM
CSA meeting-Robert Deng .pptx	(SMC)&(PROF|GRP_C)	2MB	5/4/2022 10:27:49 AM
DPM Overview-20200504.pptx	(SMC)&(PROF|GRP_C)	2MB	5/4/2022 10:28:06 AM
HoloDataSecurity-2021-Aug.pptx	(SMC)&(PROF|GRP_C)	4MB	5/4/2022 10:28:23 AM
LEAP & Countermeasures.pptx	(SMC)&(PROF|GRP_C)	2MB	5/31/2022 2:01:06 PM
LEAP - CCS 2021 - full version.pptx	(SMC)&(PROF|GRP_C)	2MB	5/31/2022 1:56:52 PM
Robert Deng EDES.pptx	(SMC)&(PROF|GRP_C)	2MB	5/31/2022 1:57:46 PM
Robert Deng-sBox.pptx	(SMC)&(PROF|GRP_C)	2MB	5/31/2022 1:58:19 PM
Sbox-New.pptx	(SMC)&(PROF|GRP_C)	2MB	5/4/2022 10:29:12 AM
全息安全2021-06-16.pptx	(SMC)&(PROF|GRP_C)	4MB	5/4/2022 10:29:42 AM

sBox Screen Shot



Path: Corporate: Search

EDESE

Name	View Policy	Size	Create Time
LEAP & Countermeasures.pptx	(SMC)&(PROF|GRP_C)	2.32MB	5/31/2022 2:01:06 PM
LEAP - CCS 2021 - full version.pptx	(SMC)&(PROF|GRP_C)	2.23MB	5/31/2022 1:56:52 PM
Robert Deng EDES.pptx	(SMC)&(PROF|GRP_C)	1.97MB	5/31/2022 1:57:46 PM
Robert Deng-sBox.pptx	(SMC)&(PROF|GRP_C)	1.93MB	5/31/2022 1:58:19 PM

Agenda

Introduction

sBox – Cloud Data Security & Privacy Platform in Zero Trust Environment

Underlying Cryptographic Techniques

Conclusion

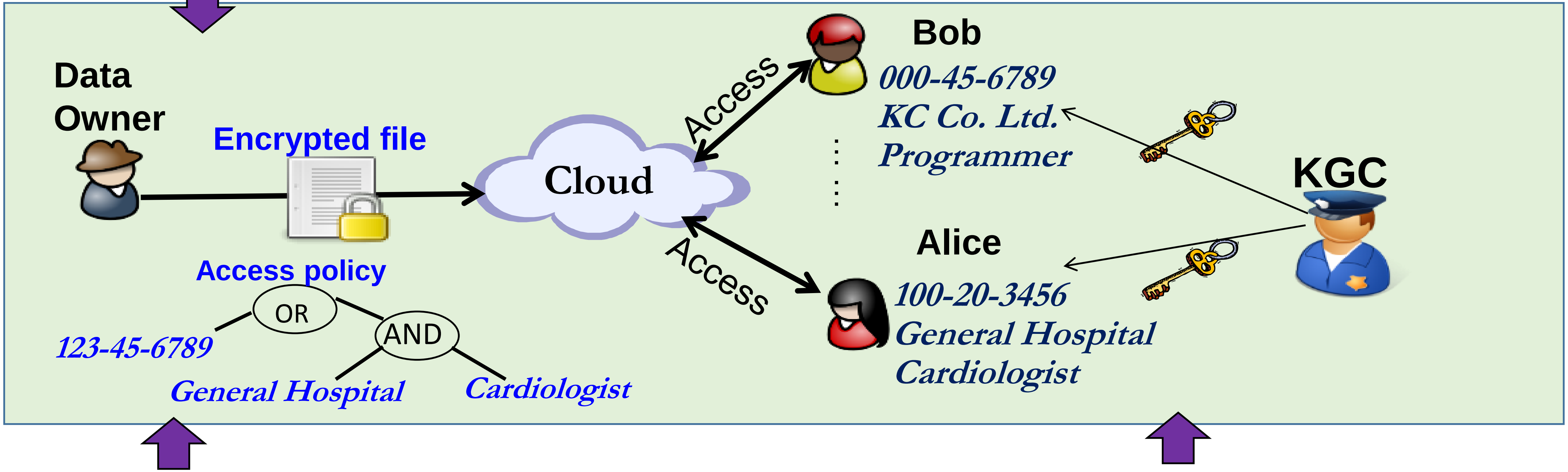
sBox’s Underlying Cryptographic Techniques

- Scalable Access Control
  - CP-ABE (Ciphertext-Policy Attributed-Based Encryption) with Outsourced Decryption [ESORICS’15 & 16, TIFS 13 & 15]
- Secure Search
  - Multiple User EDESE (Efficiently Deployable, Efficiently Searchable Encryption) [ISPEC’08, CCS’21]
- Secure Computation
  - Twin-Server based Secure Computation [TDSC’18, DSC’22, TIFS to appear]

Ciphertext-Policy Attributed-Based Encryption (CP-ABE)

[Goyal, Pandey, Sahai, and Water CCS'06]

One-to-many public key encryption



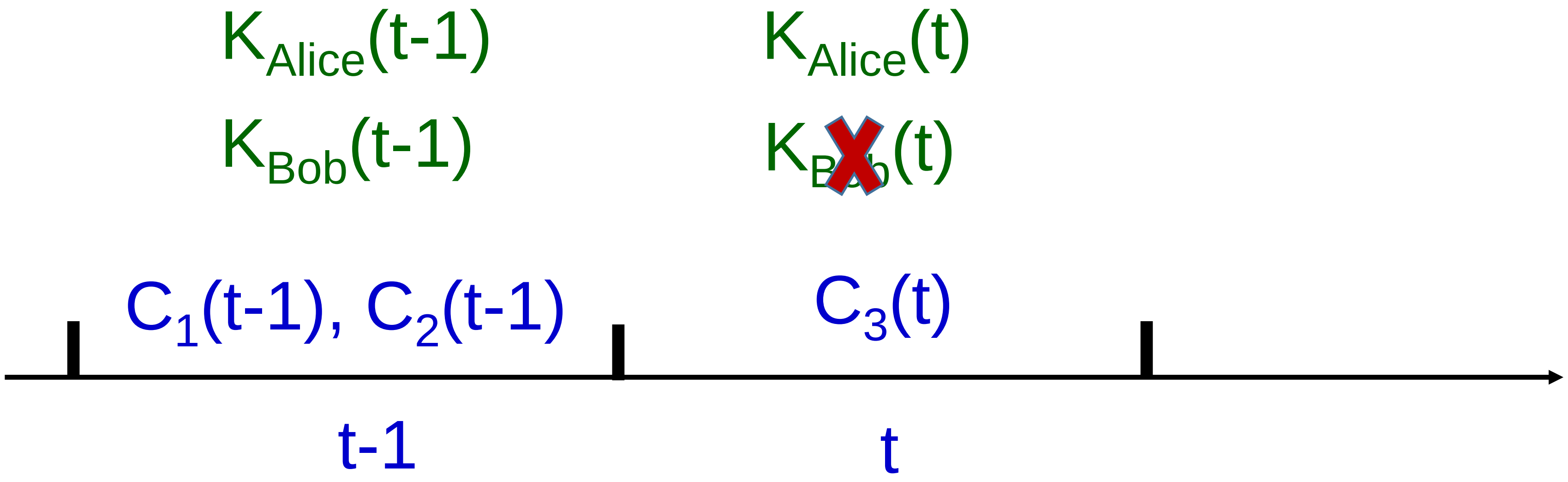
Expressive access control policies

Access control built in math

- How to perform user revocation efficiently?

ABE User Revocation - Existing Solutions

- Basic Idea
  - Time is divided into regular intervals
  - Every ciphertext is associated with a timestamp
  - A valid user’s private key is updated periodically; while revoked users will not receive key update



$K_{Alice}(t-1)$

$K_{Bob}(t-1)$

$K_{Alice}(t)$

$K_{\cancel{Bob}}(t)$

$C_1(t-1)$, $C_2(t-1)$

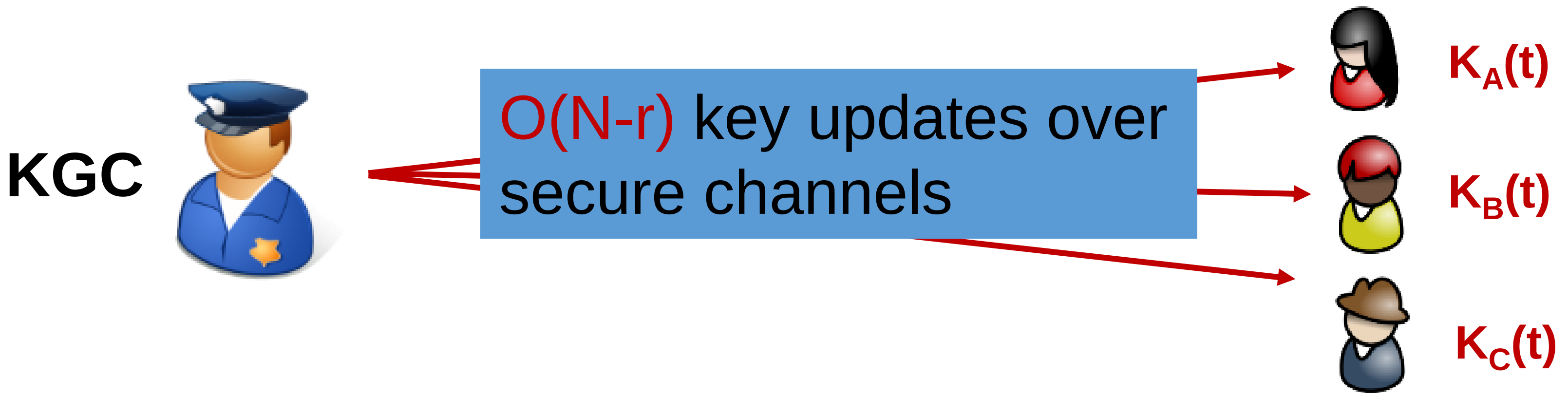
$C_3(t)$

t-1

t

ABE User Revocation - Existing Solutions (2)

- Basic approach: KGC periodically updates users' private keys over private channels [Boneh & Franklin CRYPTO'01]



KGC

O(N-r) key updates over secure channels

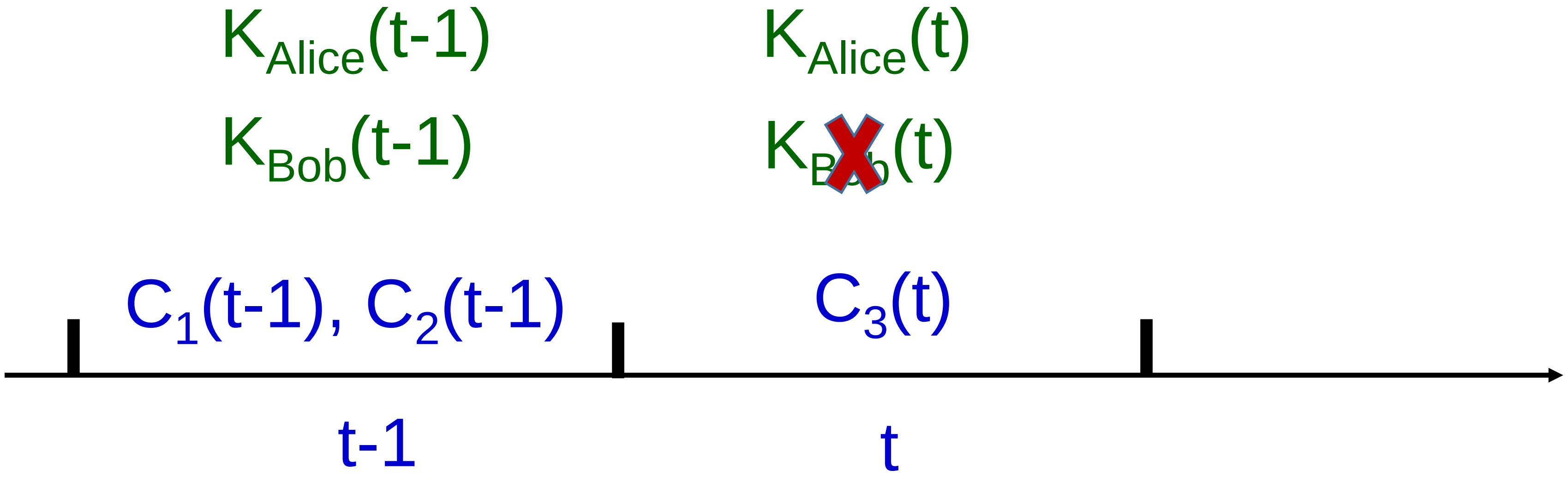
$K_A(t)$

$K_B(t)$

$K_C(t)$

- Tree-based approach: KGC periodically broadcasts key updates to users over public channels [Boldyreva, Goyal, Kumar CCS'08] [Seo & Emura PKC'13]
- Server-aided revocation: A public server handles user revocation while users are not involved in the revocation process at all [ESORICS'15; ESORICS'16, SecureComm'17]

Limitation of Existing Approaches to ABE User Revocation



$K_{Alice}(t-1)$

$K_{Bob}(t-1)$

$K_{Alice}(t)$

$K_{\cancel{Bob}}(t)$

$C_1(t-1), C_2(t-1)$

$C_3(t)$

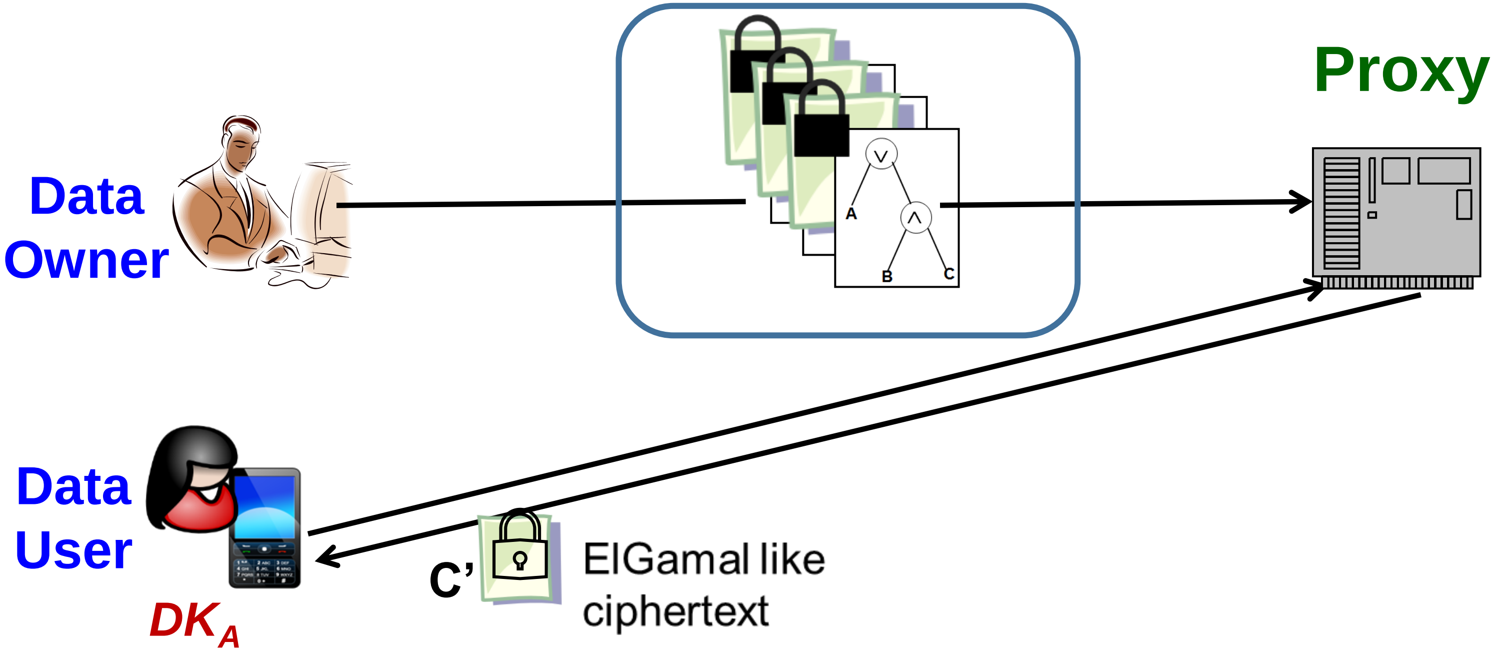
t-1

t

- Need to update C(t-1) to C(t) to prevent access by revoked users, called ciphertext delegation to storage server [Sahai, Seyalioglu and Waters Crypto'12] → **Huge computational cost**

CP-ABE with Verifiable Outsourced Decryption (CP-ABE-VOD)
[TIFS'13, TIFS'15]

- A user has a decryption key *DK* and transformation key *TK*
- To revoke a user, the proxy deletes the transformation key → assuming proxy does not collude with users



User	Transform Key
Alice	TK_A
Bob	TK_B
Carol	TK_C
David	TK_D

sBox's Underlying Cryptographic Techniques

- Scalable Access Control
  - CP-ABE (Ciphertext-Policy Attributed-Based Encryption) with Outsourced Decryption [ESORICS'15 & 16, TISF 13 & 15]
- Secure Search
  - Multiple User EDESE (Efficiently Deployable, Efficiently Searchable Encryption) [ISPEC'08, CCS'21]
- Secure Computation
  - Twin-Server based Secure Computation [TDSC'18, DSC'22, TIFS to appear]

Inverted Index for plaintext search

Keyword	Document ID
W_1	3, 4, 7, 9
W_2	1, 3, 7, 8
……	……
W_n	5, 7, 8

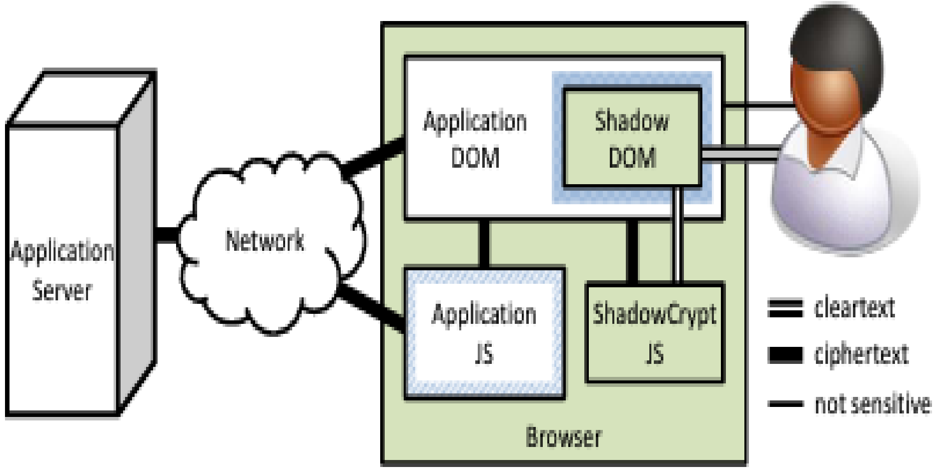
Inverted Index for searchable encryption in EDESE

Index	Document ID
$I_K(W_1)$	3, 4, 7, 9
$I_K(W_2)$	1, 3, 7, 8
……	……
$I_K(W_n)$	5, 7, 8

- EDESE search operation is the same as in plaintext search which ensures backward compatibility

Deployments of EDESE for Single User Environment

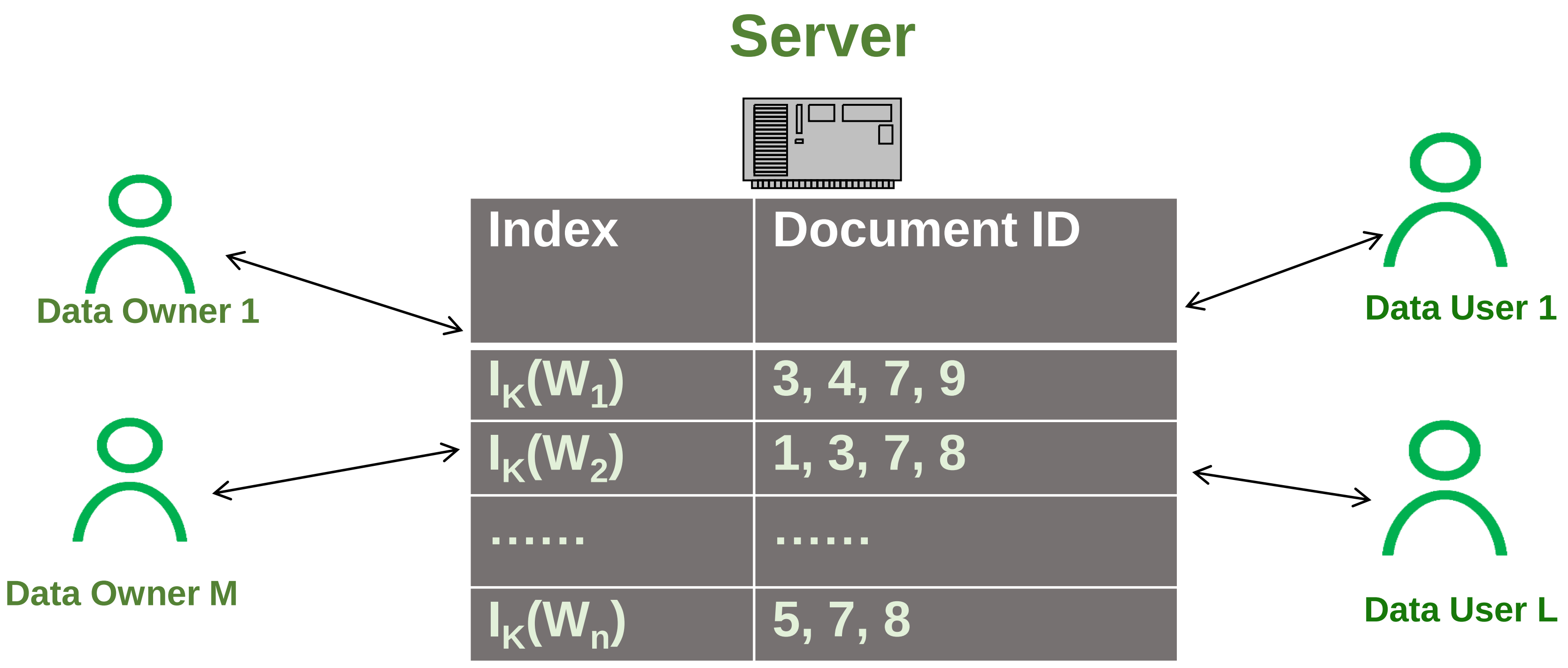
- ShaowCrypt [CCS’14]
  - ShaowCrypt E2E encrypts user data for existing web apps (Gmail, Facebook, Twitter, Reddit, etc)
- MAegis [USENIXS’14]
  - MAegis E2E encrypts user data for existing mobile apps (Gmail, Facebook Messenger, WhatsApp, etc.)



- Why EDESE?
  - “Adoption of most of the existing SE proposals requires significant rewrites. The resulting deployment and usability difficulty is an insurmountable mountain for typical users and developers” [CCS’14]

[CCS’14] He, Akhawe, Jain, Shi, Song, "Shadowcrypt: Encrypted web applications for everyone." CCS 2014
[USENIXS’14] Lau, Chung, Jang, Lee, and Boldyreva "Mimesis aegis: A mimicry privacy shield–a system’s approach to data privacy on public cloud." USENIX Security 2014

Multiuser EDESE



Server

Data Owner 1

Data Owner M

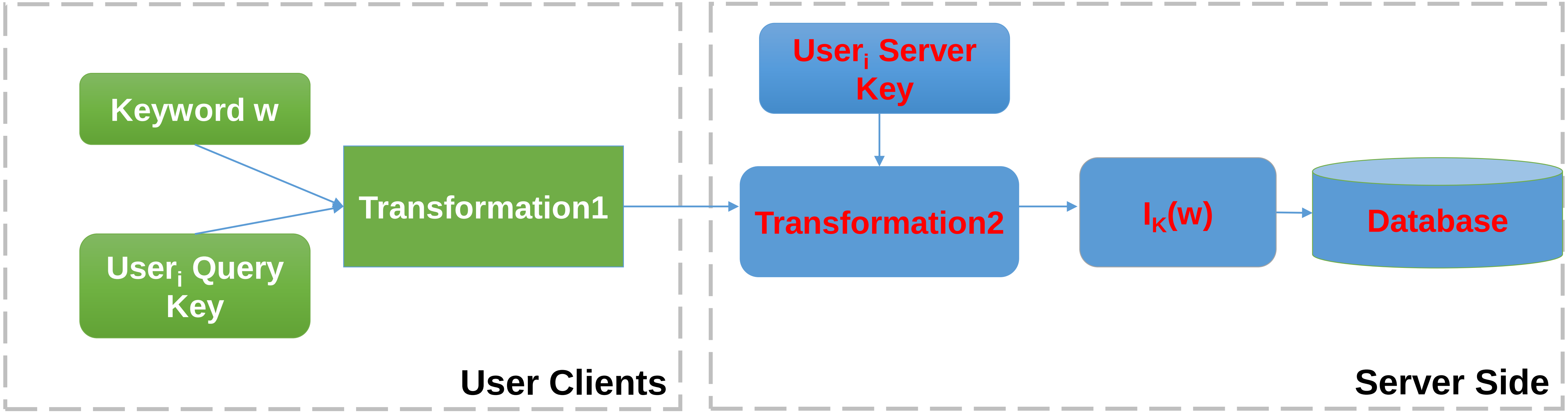
Data User 1

Data User L

Index	Document ID
$I_K(W_1)$	3, 4, 7, 9
$I_K(W_2)$	1, 3, 7, 8
……	……
$I_K(W_n)$	5, 7, 8

- Efficient user revocation is crucial for a multiuser system

Multiuser EDESE with User Revocation



Adapted from Bao, Deng, Ding, Yang, Private query on encrypted data in multi-user settings. In ISPEC 2008

Multiuser EDESE -- Properties

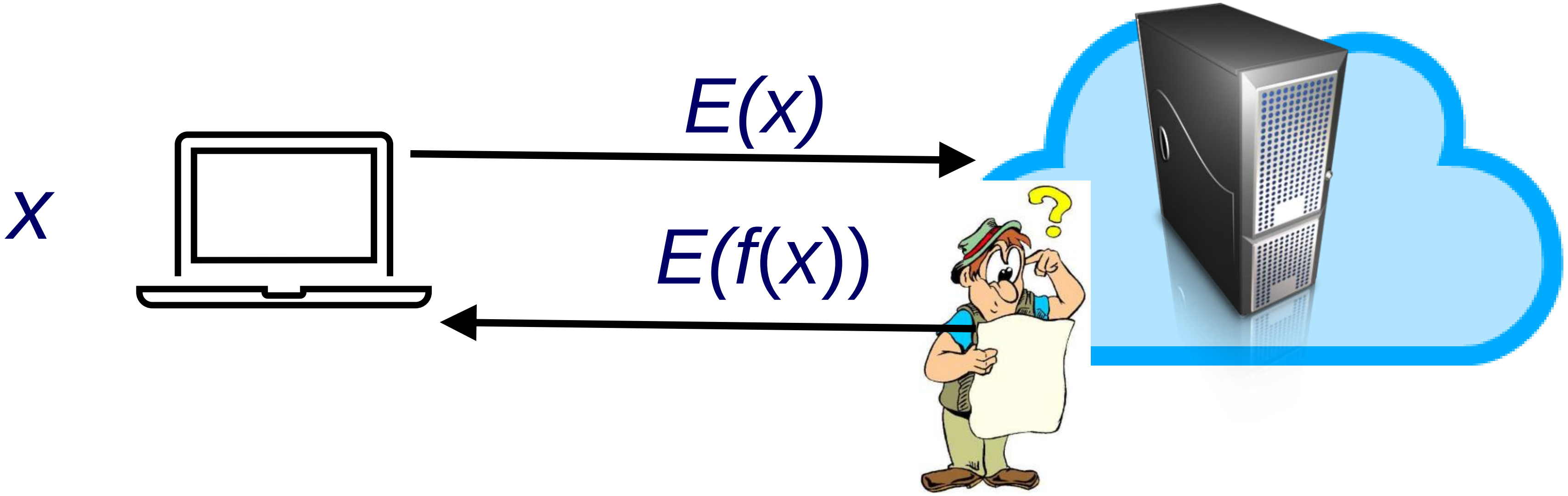
- Supporting multiple users uploading and downloading; efficient user revocation
- Keyword index and token secure against keyword dictionary attack
- Efficient search, e. g., log(n)
- But subject to LEAP attack [CCS’21] (query/document recovery attack assuming attacker knows a subset of the documents)

Ning, Huang, Poh, Yuan, Li, Weng, Deng, Leakage-abuse attack on efficiently deployable, efficiently searchable encryption with partial known dataset, CCS 2021.

sBox’s Underlying Cryptographic Techniques

- Scalable Access Control
  - CP-ABE (Ciphertext-Policy Attributed-Based Encryption) with Outsourced Decryption [ESORICS’15 & 16, TISF 13 & 15]
- Secure Search
  - Multiple User EDESE (Efficiently Deployable, Efficiently Searchable Encryption) [ISPEC’08, CCS’21]
- Secure Computation
  - Twin-Server based Secure Computation [TDSC’18, DSC’22, TIFS to appear]

Fully Homomorphic Encryption (FHE)

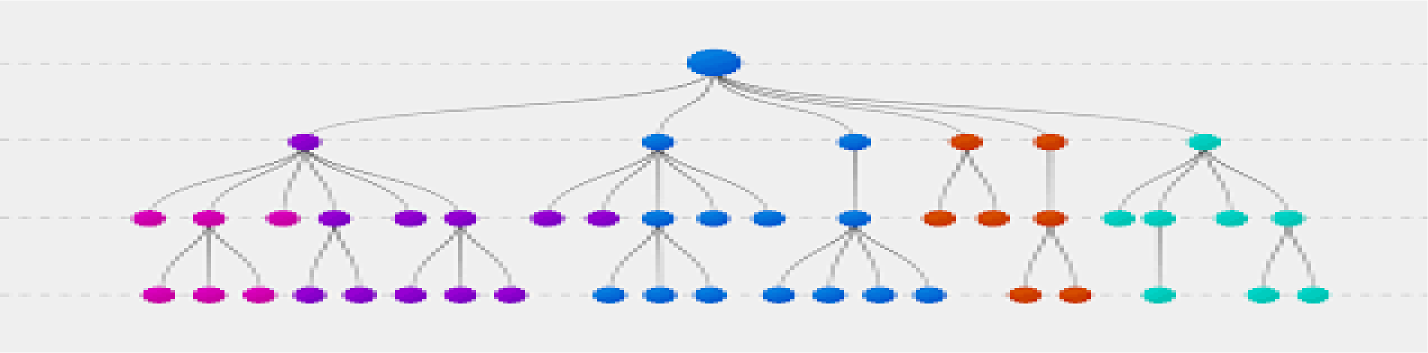


- Data owner privately outsources computation to an untrusted server
- Server performs computation but never gains access to input, intermediate result, and final output

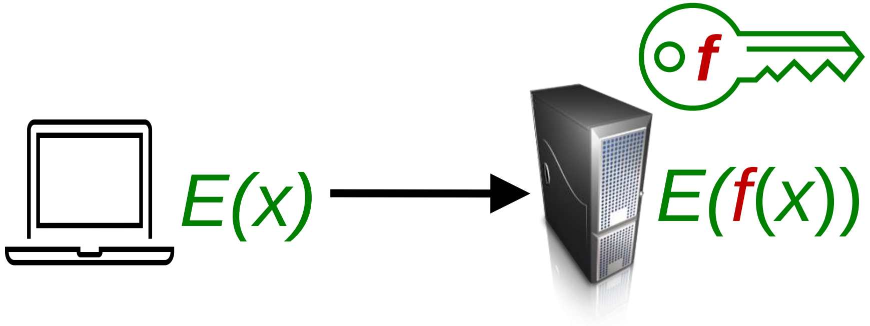
Limitations of FHE

- Server has no access to intermediate or final result
  - E. g., Not possible for a server to run spam-detection algorithm on encrypted emails

- Server cannot follow data-dependent flows
  - Encrypted array search/sorting
  - Encrypted decision tree



Functional Encryption

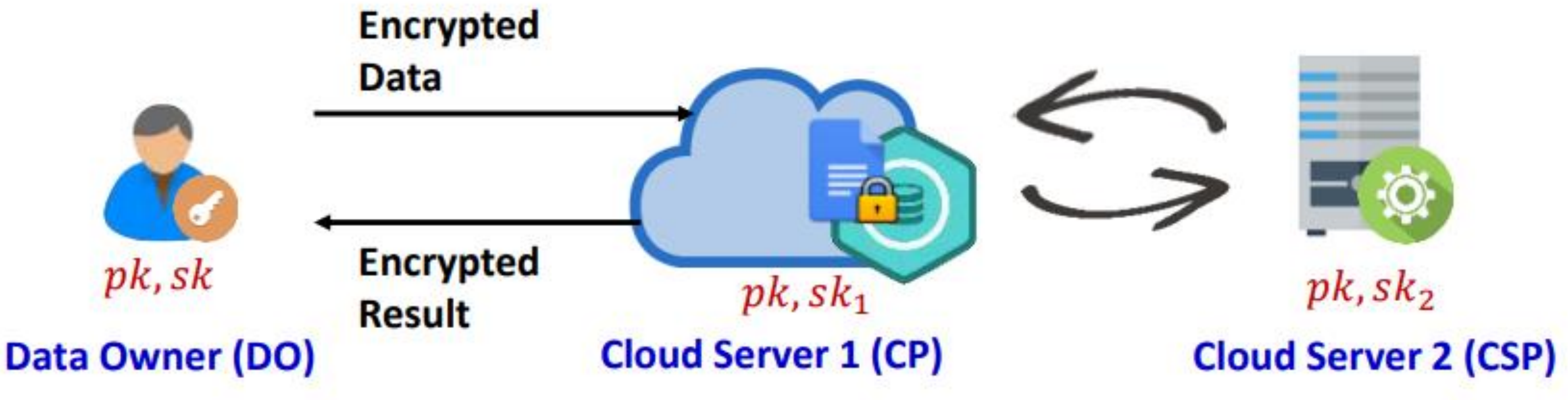


Server can access output, but performance is in general worse than FHE

Our objective is design secure computation schemes that

- Give server access to intermediate result and final output if required
- With performance much superior to FE

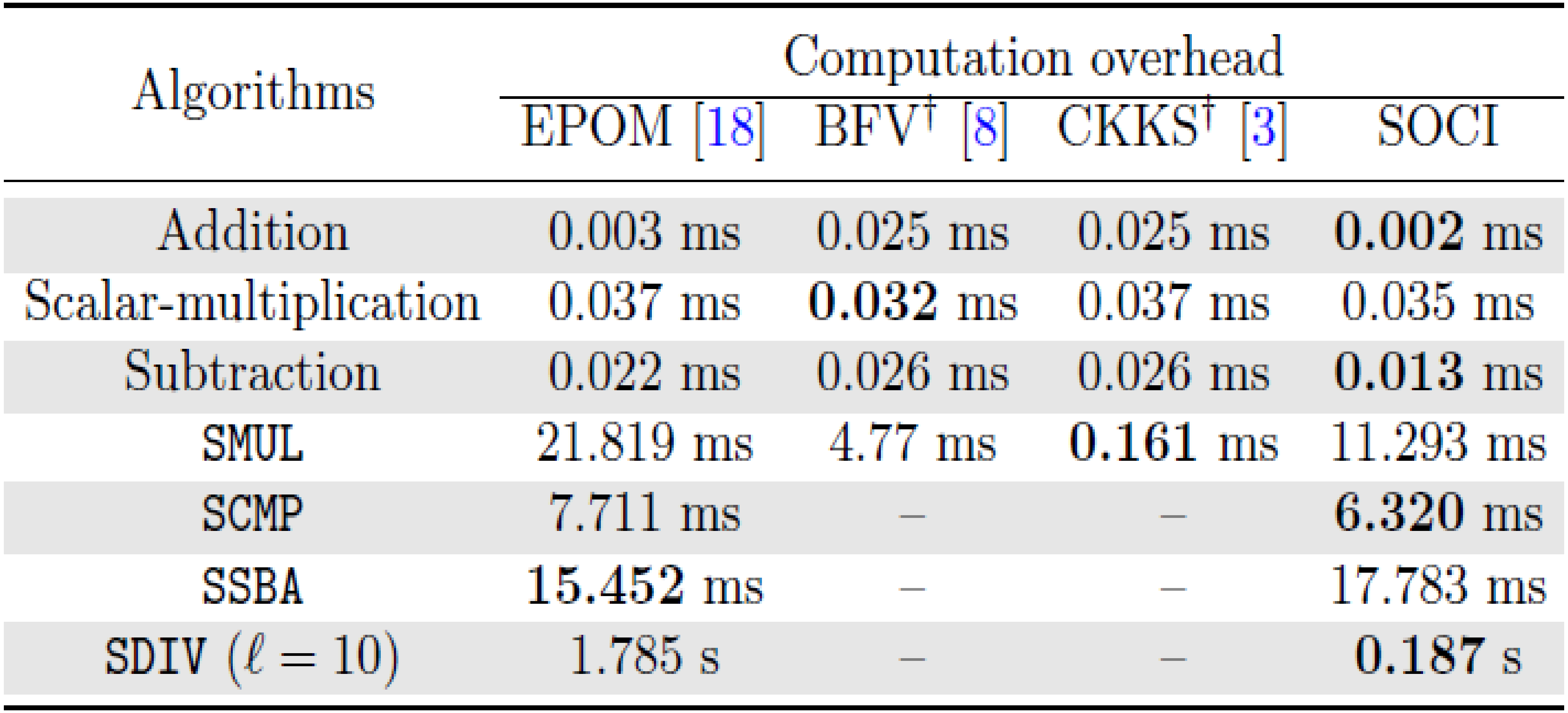
Twin-Server based Secure Computation



- **Assumption:** CP and CSP don't collude
- **Paillier encryption:** CP and CSP each has a partial private key
- **CP and CSP:** interact to perform secure computations; **can jointly access intermediate result and final output**

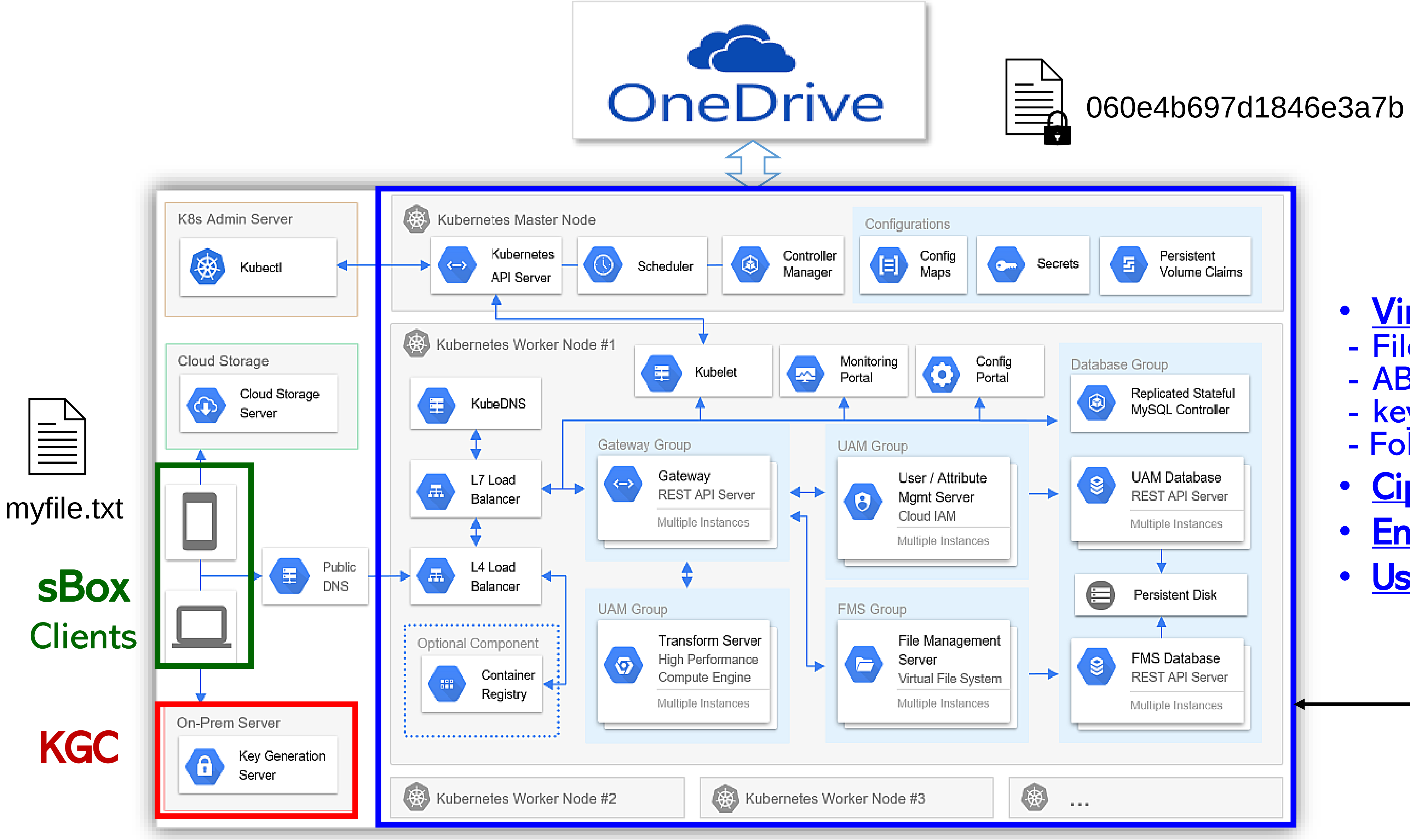
Liu, Choo, Deng , Lu, Weng, Efficient and privacy-preserving outsourced calculation of rational numbers. IEEE TDSC, Jan-Feb 2018.
Zhao, Yuan, Liu, Wu, Pang, Deng, "SOCI: A toolkit for secure outsourced computation on integers", IEEE TIFS to appear
Zhao. Li, Liu, Pang, Deng, "FREED: An efficient privacy-preserving solution for person re-identification", IEEE DSC 2022

Performance (80-bit security)



Algorithms	Computation overhead			
	EPOM [18]	BFV† [8]	CKKS† [3]	SOCI
Addition	0.003 ms	0.025 ms	0.025 ms	**0.002** ms
Scalar-multiplication	0.037 ms	**0.032** ms	0.037 ms	0.035 ms
Subtraction	0.022 ms	0.026 ms	0.026 ms	**0.013** ms
SMUL	21.819 ms	4.77 ms	**0.161** ms	11.293 ms
SCMP	7.711 ms	–	–	**6.320** ms
SSBA	**15.452** ms	–	–	17.783 ms
SDIV ($\ell = 10$)	1.785 s	–	–	**0.187** s

sBox Architecture & Implementation



- Virtual File System
  - File name→ pseudo name
  - ABE access policy
  - keyword index
  - Folder access permissions
- Ciphertext transformation
- Encrypted keyword search
- User revocation

sBox
server
cluster

Agenda

Introduction

sBox – Cloud Data Security & Privacy Platform in Zero Trust Environment

Underlying Cryptographic Techniques

Conclusion

Conclusion

- Many novel cryptographic techniques for data protection have been proposed in the literature
  - Theoretical results, piecemeal solutions
  - Limited in usability and efficiency on their own
- Need to carefully select and customize crypto algorithms, and seamlessly integrate crypto & system to balance security, efficiency, and usability, and to maintain backward compatibility

Conclusion (2)

- **sBox** is a cloud data security & privacy platform for enterprise users in zero trust environment, which
  - Integrates ABE-VOD (for access control) and multiuser EDESE (for secure search) with a unified user revocation framework
  - Supports 2 layers of access control: system level and crypto level
  - Supports Twin-Server based Secure Computation (next step)
- In general, much more efforts are required to bridge the gap between crypto research and practical applications (hence, there are many research opportunities along this direction)

Thank you!