UNIVERSITY
OF TWENTE.

SECURE CLOUD COMPUTING

INTRODUCTION AND KEY MANAGEMENT SERVICE

CONTENT

- Organization of this Course
- Definition of Cloud Computing
  - Characteristics
  - Service Models
  - Deployment Models
- Amazon’s Key Management Service
  - Detailed discussion
- Internal Attackers in Cloud Computing
  - Protection Goals

Organizational Stuff

Florian Hahn
Assistant Professor @ SCS Group
https://people.utwente.nl/f.w.hahn
f.w.hahn@utwente.nl

Jair Santanna
Assistant Professor @ DACS Group
and CloudSecurity@Northwave
https://people.utwente.nl/j.j.santanna
j.j.santanna@utwente.nl

7. September	Introduction	
14. September	Encrypted Databases	Assignment 1
21. September	Advanced Techniques for Encrypted Storage	
28. September	Cloud Security from an End-User Perspective	Assignment 2
5. October	How to Deploy Security to Cloud End-Users	
11. October	Hardware-Aided Computation over Encrypted Data	Assignment 3
18. October	Outsourced Computation over Encrypted Data	
6. November	**Exam**	

Organizational Stuff

All seven lectures are given online via Canvas Conference and are recorded

3 Assignments during the course

- Due to high number of participants: in groups of 2 (organize yourselves)

Final exam (planned as written closed-book exam)

  - In case this is not possible due to Corona: Homework with oral examination afterwards

Final grade: 70% exam + 3 * (10% assignment)

7. September	Introduction	
14. September	Encrypted Databases	Assignment 1
21. September	Advanced Techniques for Encrypted Storage	
28. September	Cloud Security from an End-User Perspective	Assignment 2
5. October	How to Deploy Security to Cloud End-Users	
11. October	Hardware-Aided Computation over Encrypted Data	Assignment 3
18. October	Outsourced Computation over Encrypted Data	
6. November	**Exam**	

What is Cloud Computing?

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of

- five essential characteristics,
- three service models,
- and four deployment models. ”

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

Essential Characteristics of CC

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

The Cloud Allowed Us To Make Our
Server Room Into A Wine Cellar.

https://www.biositgroup.com/dont-need-your-business-server-room-anymore

Service Models

Software-as-a-Service:

- […] use the **provider's applications** running on a cloud infrastructure.

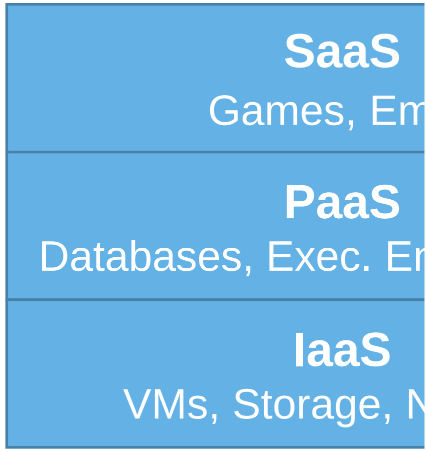
Platform-as-a-Service:

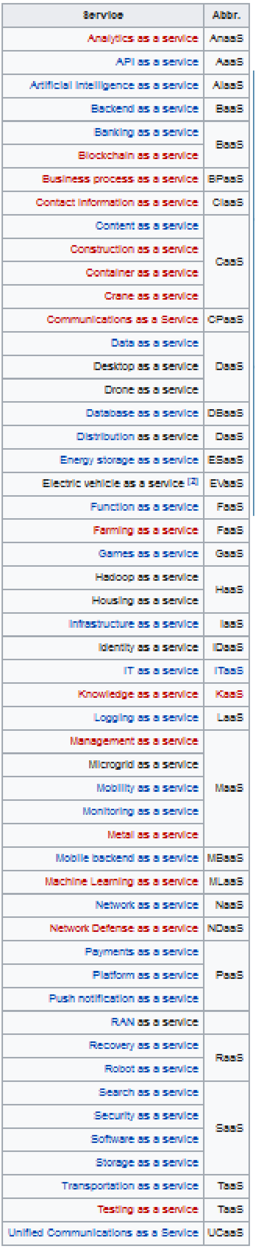
- […] deploy onto the cloud infrastructure **consumer-created or acquired applications** created using programming languages, libraries, services, and tools supported by the provider.

Infrastructure-as-a-Service:

- […] provision **processing, storage, networks, and other fundamental computing resources** where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

In recent years EaaS: Everything-as-a-Service

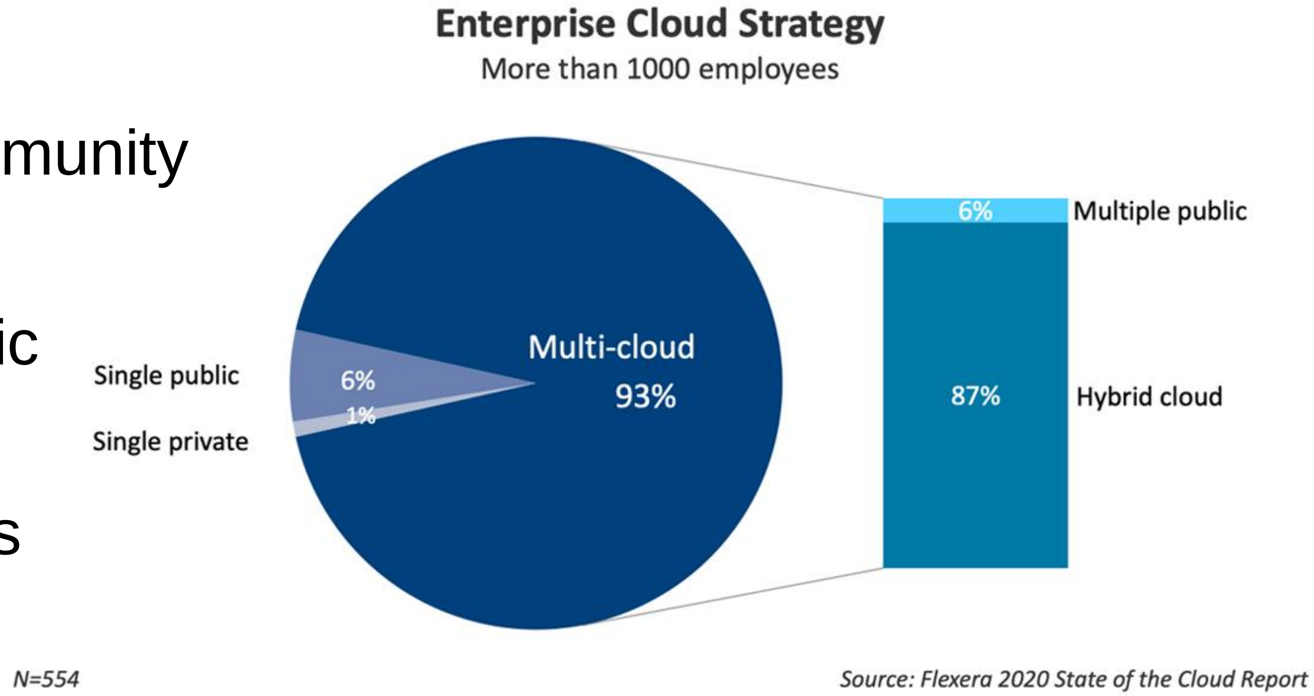




Service	Abbr.
Analytics as a service	AnaaS
API as a service	AaaS
Artificial Intelligence as a service	AIaaS
Backend as a service	BaaS
Banking as a service	BaaS
Blockchain as a service	
Business process as a service	BPaaS
Contact Information as a service	CIaaS
Content as a service	CaaS
Construction as a service	
Container as a service	
Crane as a service	
Communications as a Service	CPaaS
Data as a service	DaaS
Desktop as a service	
Drone as a service	
Database as a service	DBaaS
Distribution as a service	DaaS
Energy storage as a service	ESaaS
Electric vehicle as a service [2]	EVaaS
Function as a service	FaaS
Farming as a service	FaaS
Games as a service	GaaS
Hadoop as a service	HaaS
Housing as a service	
Infrastructure as a service	IaaS
Identity as a service	IDaaS
IT as a service	ITaaS
Knowledge as a service	KaaS
Logging as a service	LaaS
Management as a service	MaaS
Microgrid as a service	
Mobility as a service	
Monitoring as a service	
Metal as a service	
Mobile backend as a service	MBaaS
Machine Learning as a service	MLaaS
Network as a service	NaaS
Network Defense as a service	NDaaS
Payments as a service	PaaS
Platform as a service	
Push notification as a service	
RAN as a service	
Recovery as a service	RaaS
Robot as a service	
Search as a service	SaaS
Security as a service	
Software as a service	
Storage as a service	
Transportation as a service	TaaS
Testing as a service	TaaS
Unified Communications as a Service	UCaaS

Cloud Deployment Models

1. Private Cloud:
   - Exclusive use by single organization
2. Community Cloud:
   - Exclusive use by specific community
3. Public Cloud
   - Open use by the general public
4. Hybrid Cloud
   - Composition of distinct models



Enterprise Cloud Strategy

More than 1000 employees

Source: Flexera 2020 State of the Cloud Report

Why is Cloud Security Relevant?

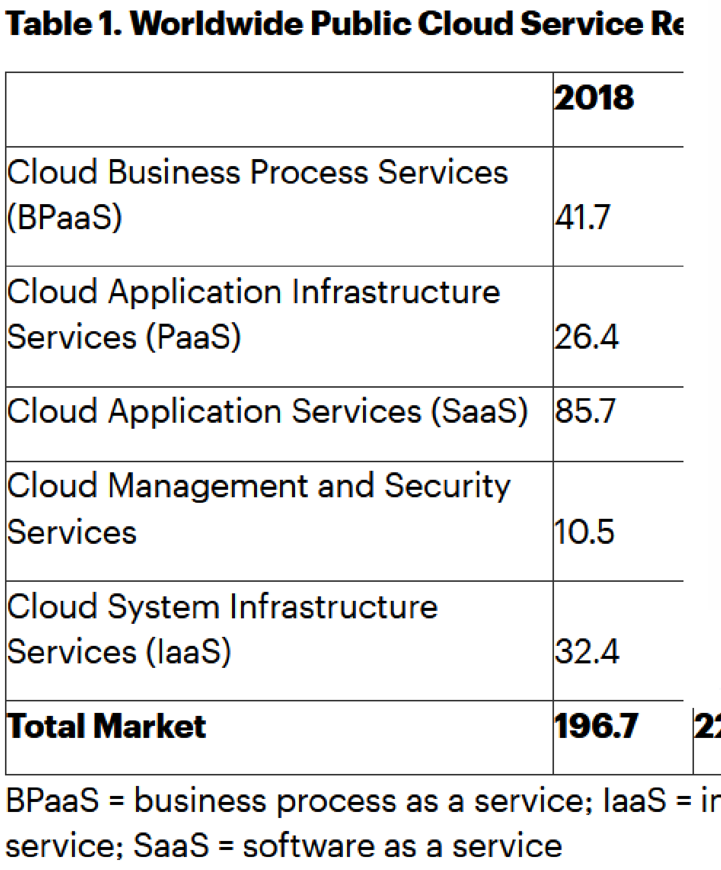
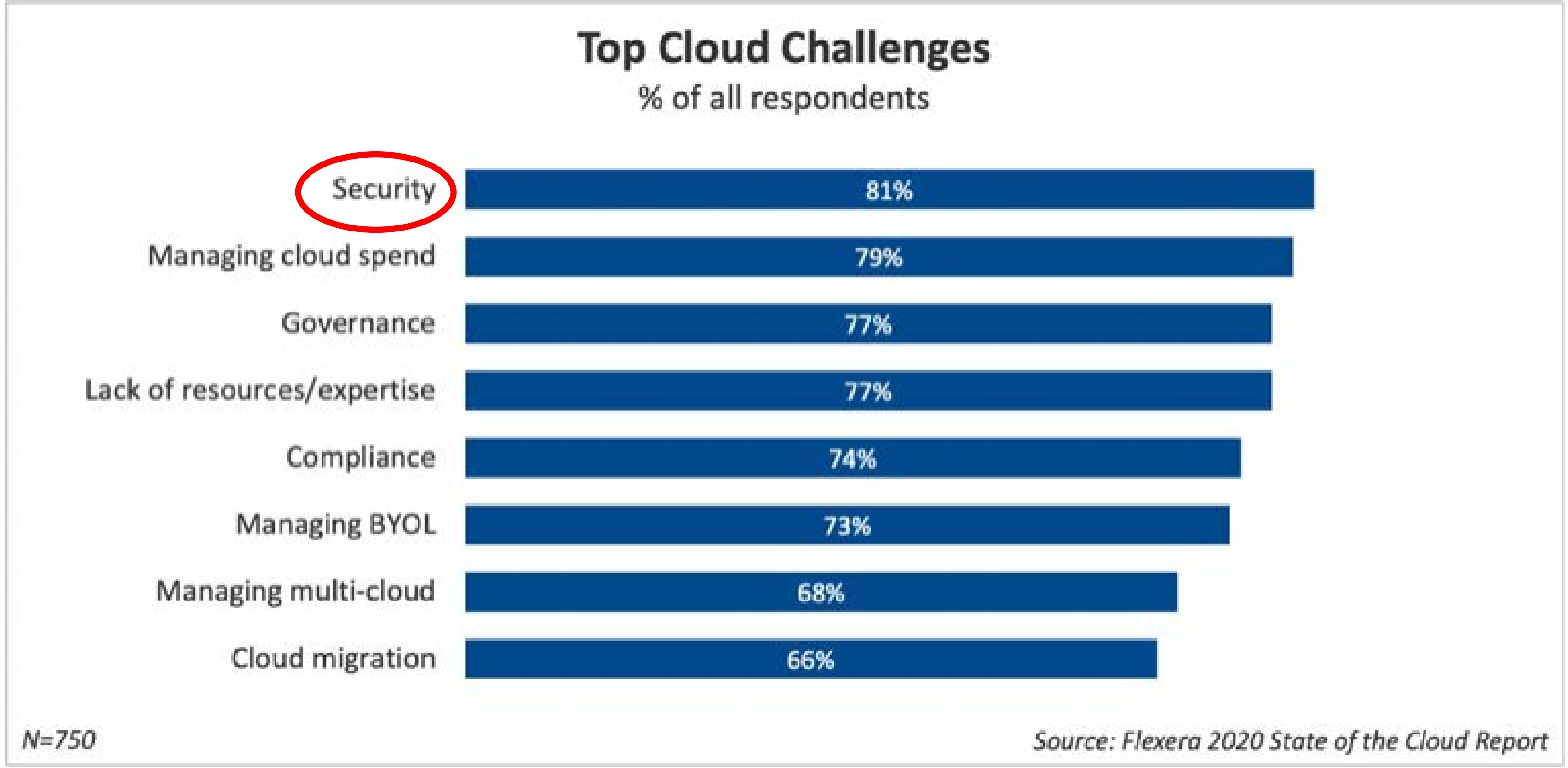


Table 1. Worldwide Public Cloud Service Re

	2018				
Cloud Business Process Services (BPaaS)	41.7				
Cloud Application Infrastructure Services (PaaS)	26.4				
Cloud Application Services (SaaS)	85.7				
Cloud Management and Security Services	10.5				
Cloud System Infrastructure Services (IaaS)	32.4				
Total Market	**196.7**	**227.8**	**266.4**	**308.5**	**354.6**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service

Source: gartner.com



Source: Flexera 2020 State of the Cloud Report

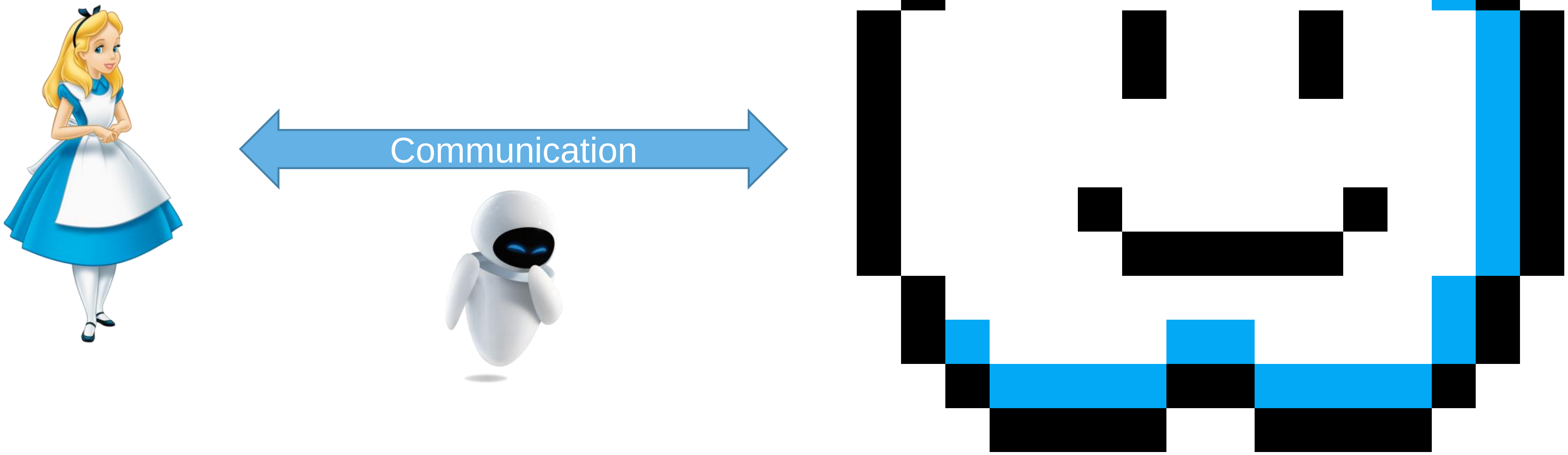
Figure 33. Top cloud challenges for all organizations

UNIVERSITY OF TWENTE.

External Adversaries…

… on the communication:

- TLS
- Network Security

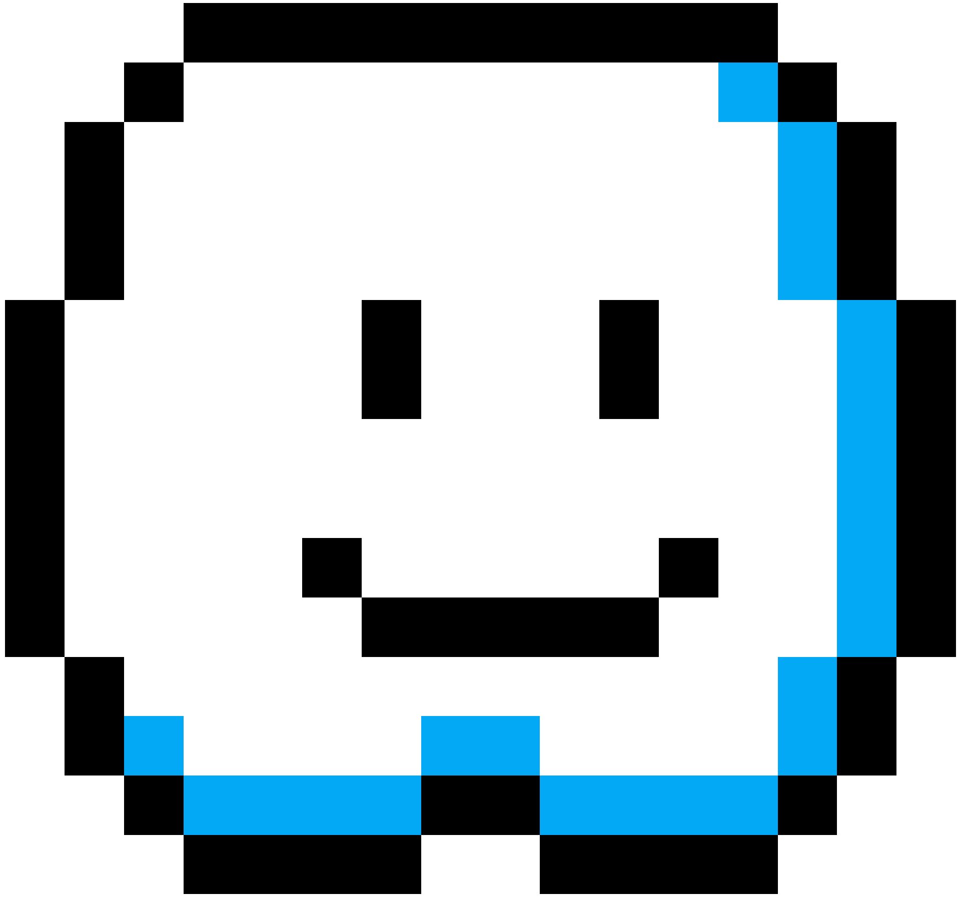


External Adversaries…

… on the cloud system:

- OS security (host and guest)
- Firewalls and IDS
- Monitoring

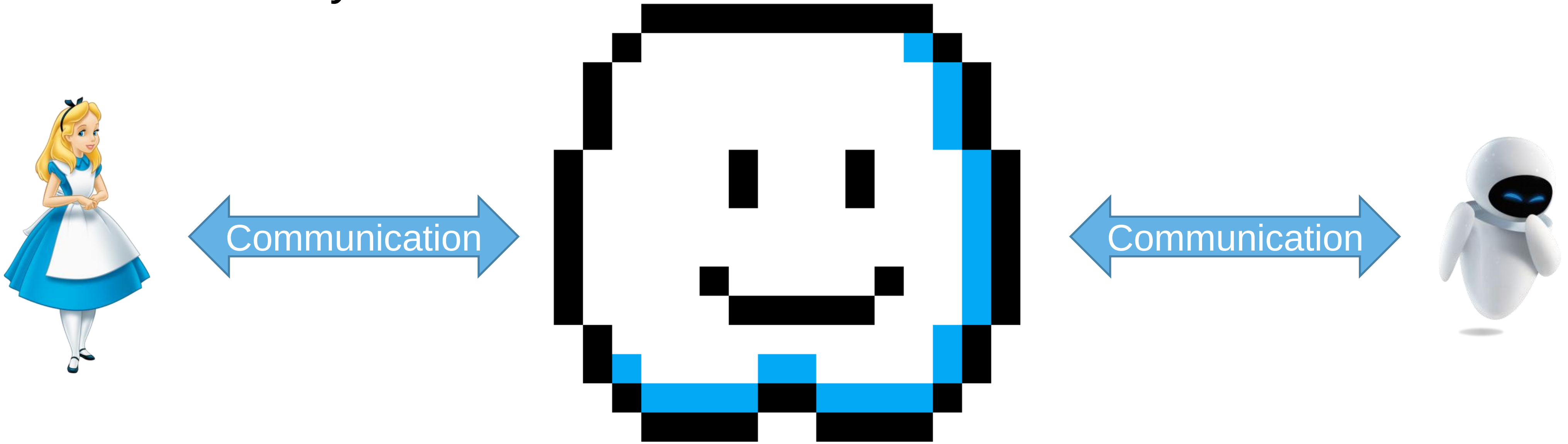
Communication



Co-tenant Adversaries…

… using the same cloud service:

- Isolation
- Sandboxing
- Monitoring
- Hardware Security Modules



AWS KMS: Security Service in the Cloud

Amazon Web Services (AWS)

- AWS Key Management Service (KMS)
- Amazon promises the following benefits:
  - **Fully Managed:** access control enforced by user while Amazon handles durability and physical security
  - **Centralized Key Management:** single control point to manage cryptographic keys
  - **Manage encryption for AWS services:** well integrated with AWS services
  - **Encrypt data in your applications:** via APIs
  - **Digitally Sign data:** using asymmetric crypto, but secret key is stored in HSM
  - **Low cost:** charged by numbers of keys stored
  - **Security:** by hardware security modules
  - **Compliance:** via certifications
  - **Built-in auditing:** requests are logged to CloudTrail

AWS KMS: Crypto Primitives

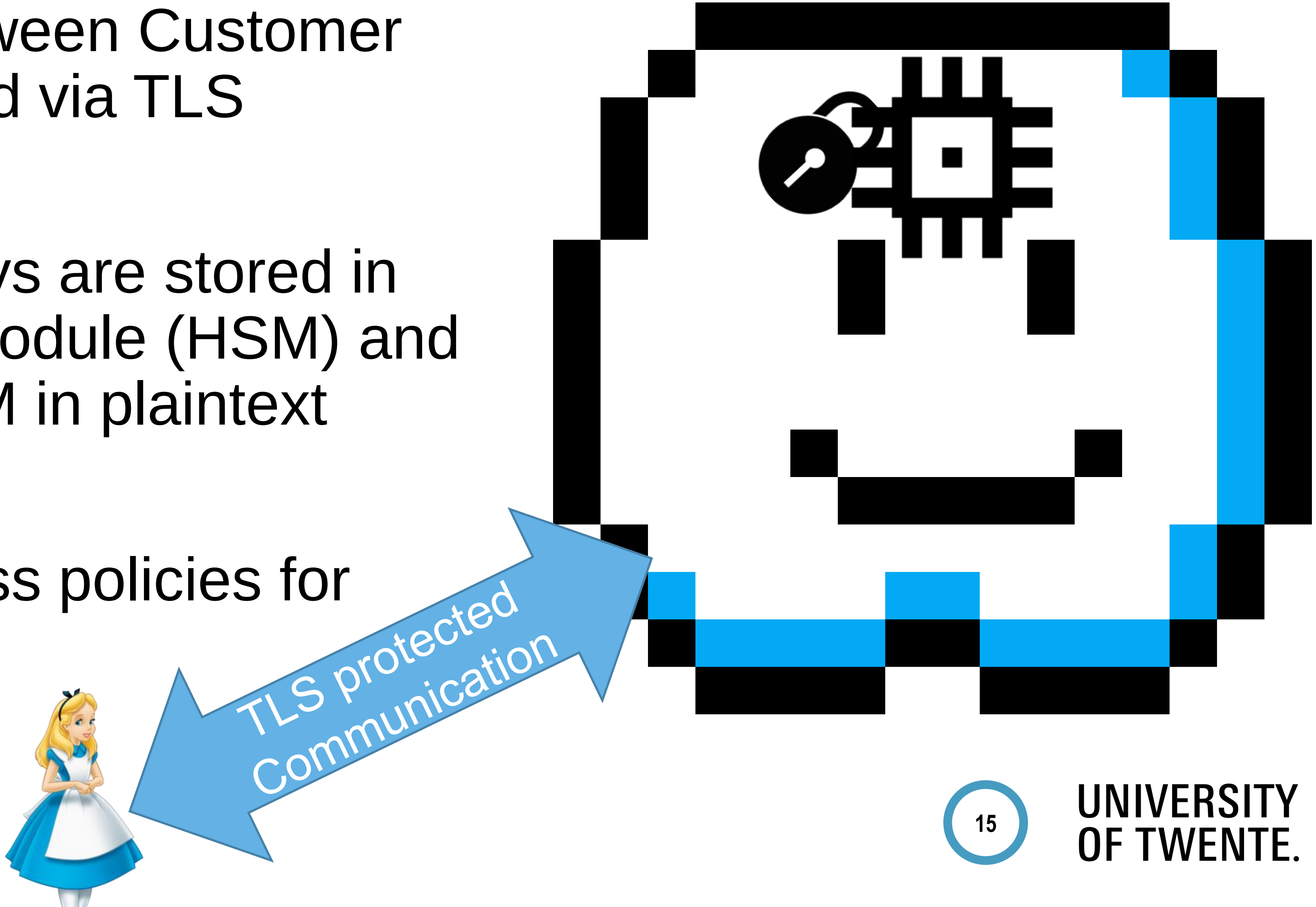
- Random Bit Generator
  - Seeded with 384 bits randomness
- Symmetric Encryption
  - AES-GCM 256
    - AEAD authenticated encryption with associated data
- Key Derivation Function
  - HMAC with SHA256 in counter mode
- Envelope Encryption
  - Encrypt Payload with data key; encrypt data key with key encryption key
- Asymmetric Encryption
  - RSA
- Digital Signatures
  - Elliptic Curve Digital Signature Algorithm (ECDSA)
- Key Establishment / Exchange Protocols
  - Diffie-Hellmann Key Exchange

AWS KMS: High level concept

Communication between Customer and Cloud is secured via TLS

Sensitive master keys are stored in hardware security module (HSM) and never leave the HSM in plaintext

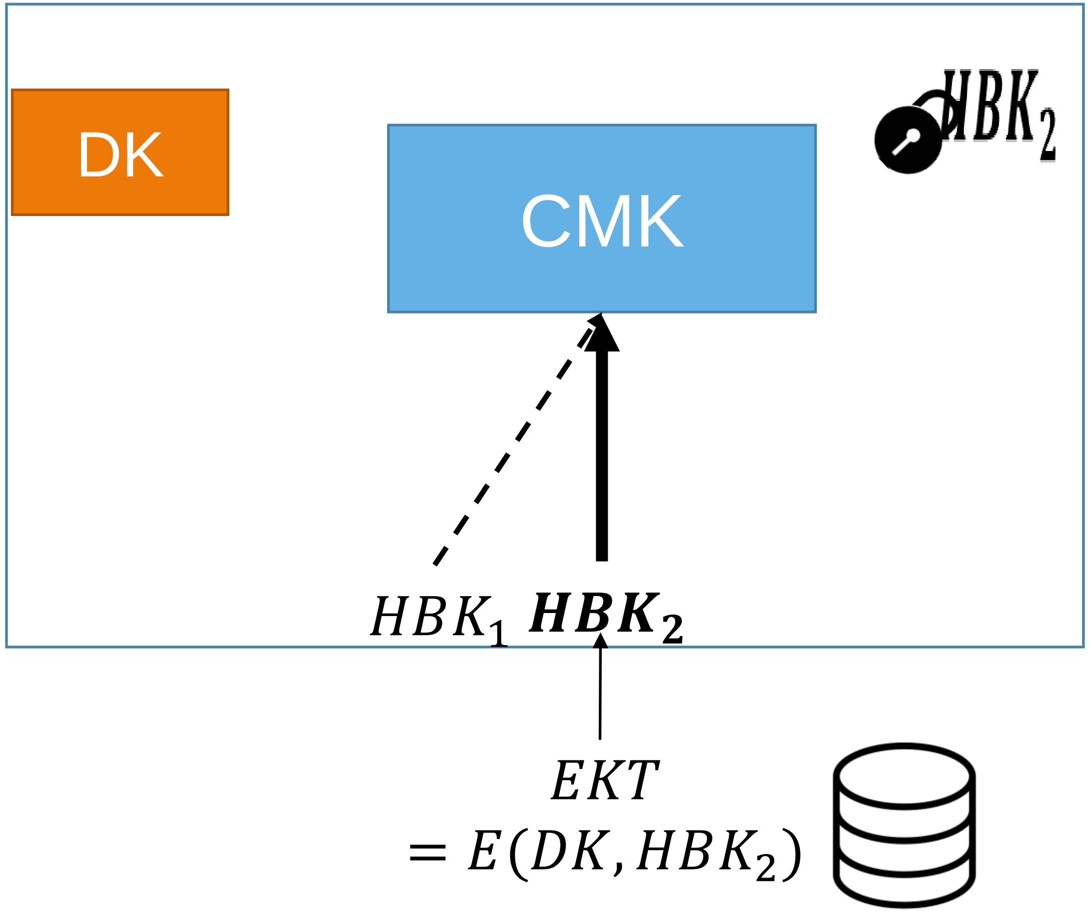
HSM enforces access policies for stored keys



AWS KMS: Customer Master Key

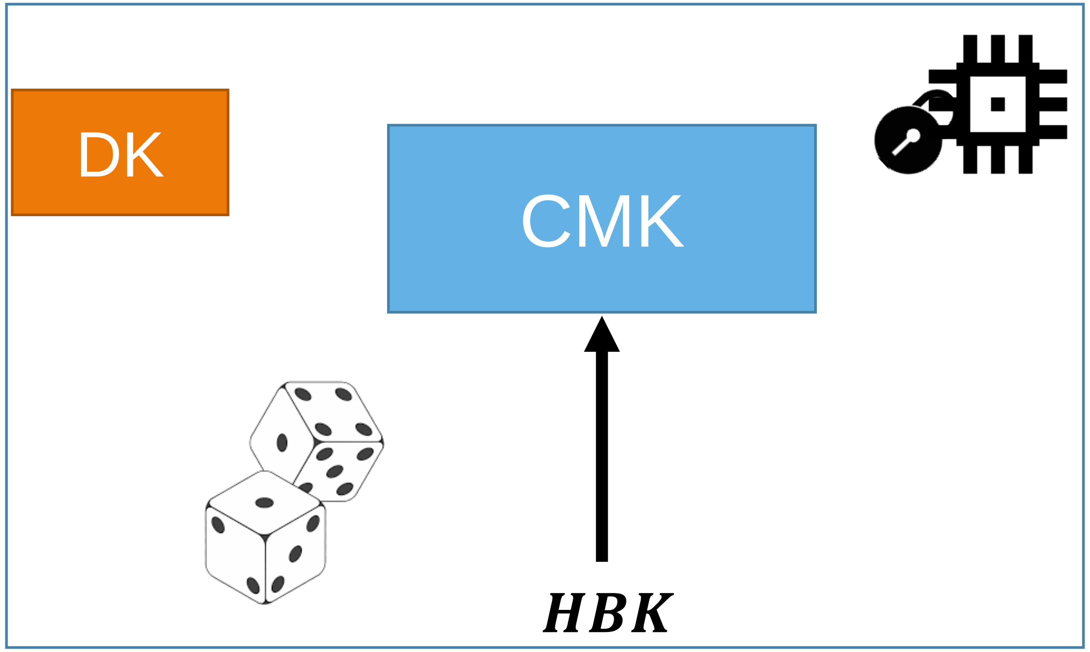
Customer Master Key (CMK)

- Logical placeholder for a real key: HSM backing key (HBK)
- Different HBK versions can be associated with same CMK
- Only encrypted version is stored outside of HSM on highly durable storage
- Exported Key Token (EKT): encrypted HBK using HSM managed domain keys (DK)



AWS KMS: Generating an HBK

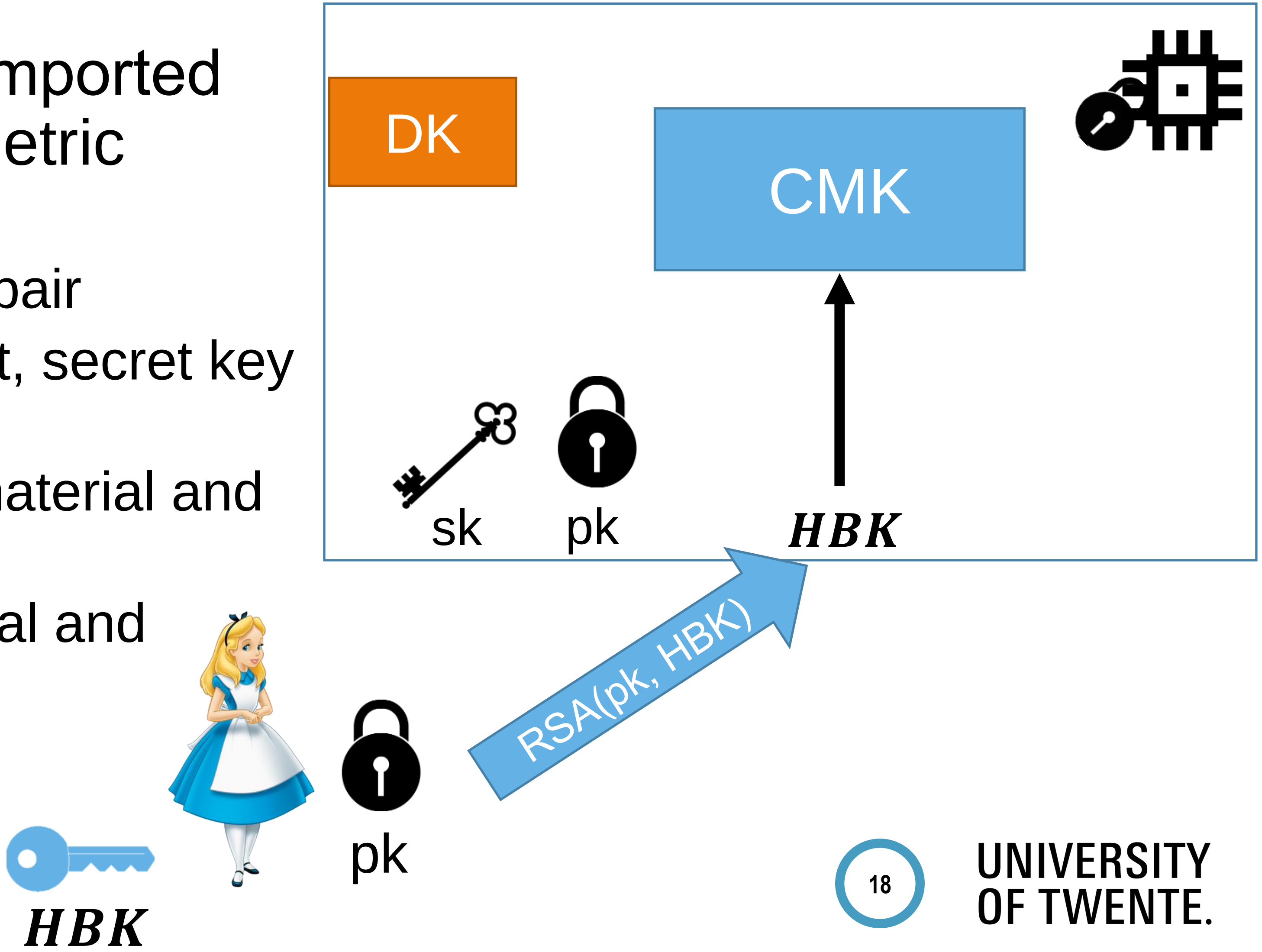
HBK can either be generated in HSM…



AWS KMS: Generating an HBK

…or key material can be imported by customer using asymmetric crypto

- HSM generates RSA keypair
- Public key is sent to client, secret key remains in HSM
- Customer encrypts key material and sends it back to HSM
- HSM decrypts key material and stores it as HBK



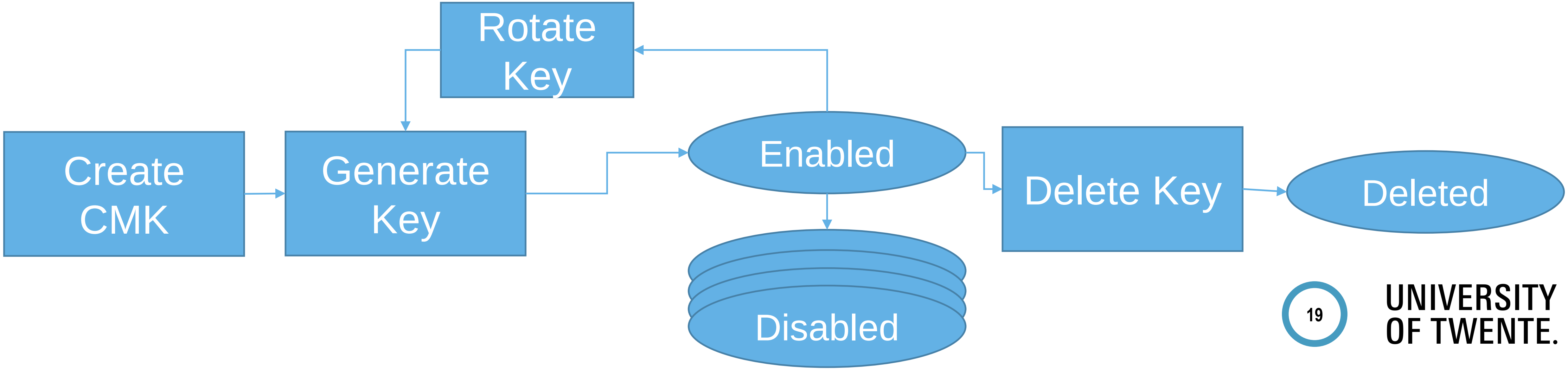
AWS KMS: CMK lifecycle

CMKs can be rotated:

- Disabled keys can still be used for decryption

CMKs can be deleted:

- Internally, CMK is completely disabled 7 days before actual deletion



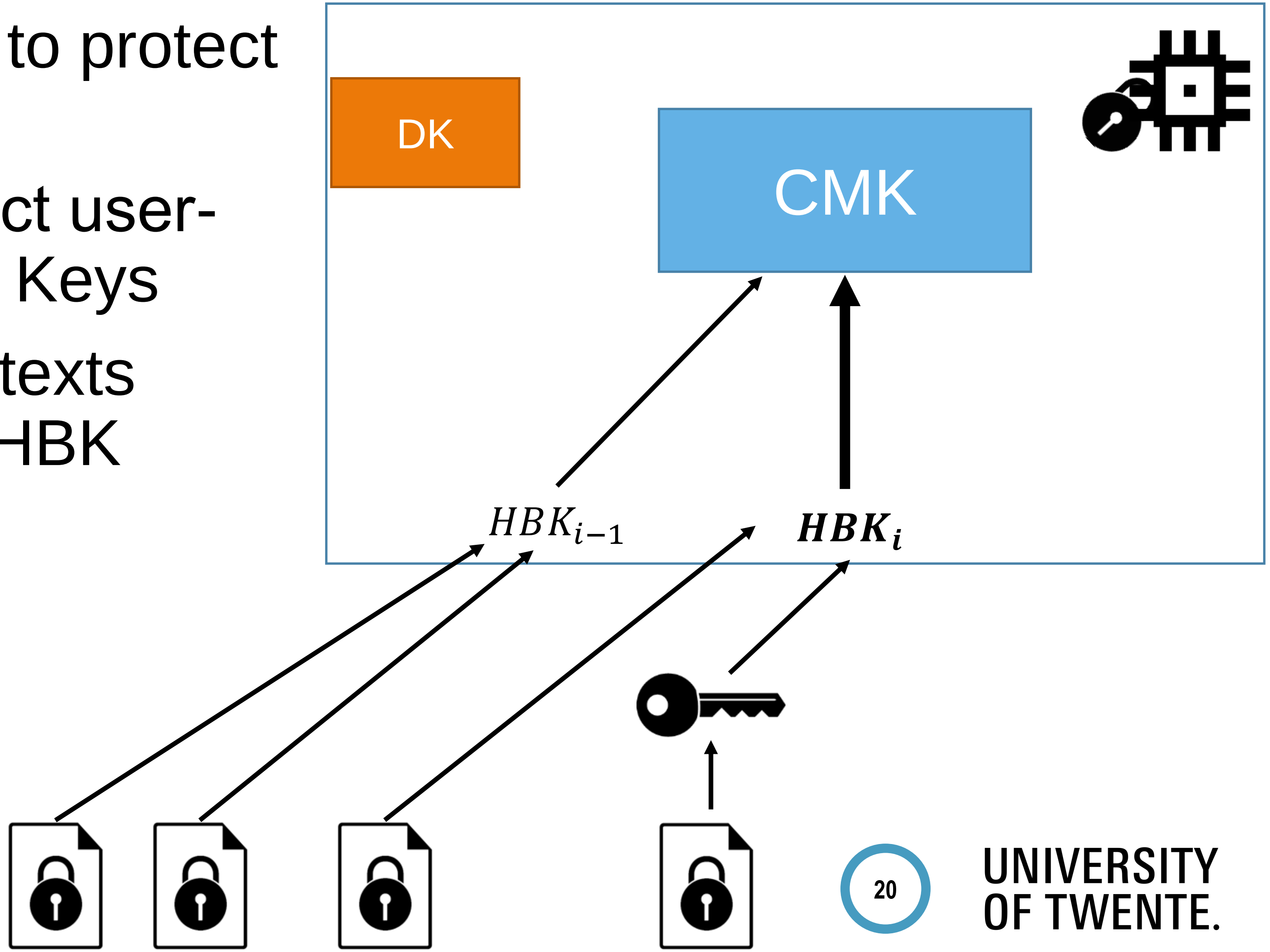
UNIVERSITY OF TWENTE.

AWS KMS: Key Hierarchy

CMK can be used directly to protect information…

… or can be used to protect user-generated Customer Data Keys

- And there may be ciphertexts encrypted with disabled HBK



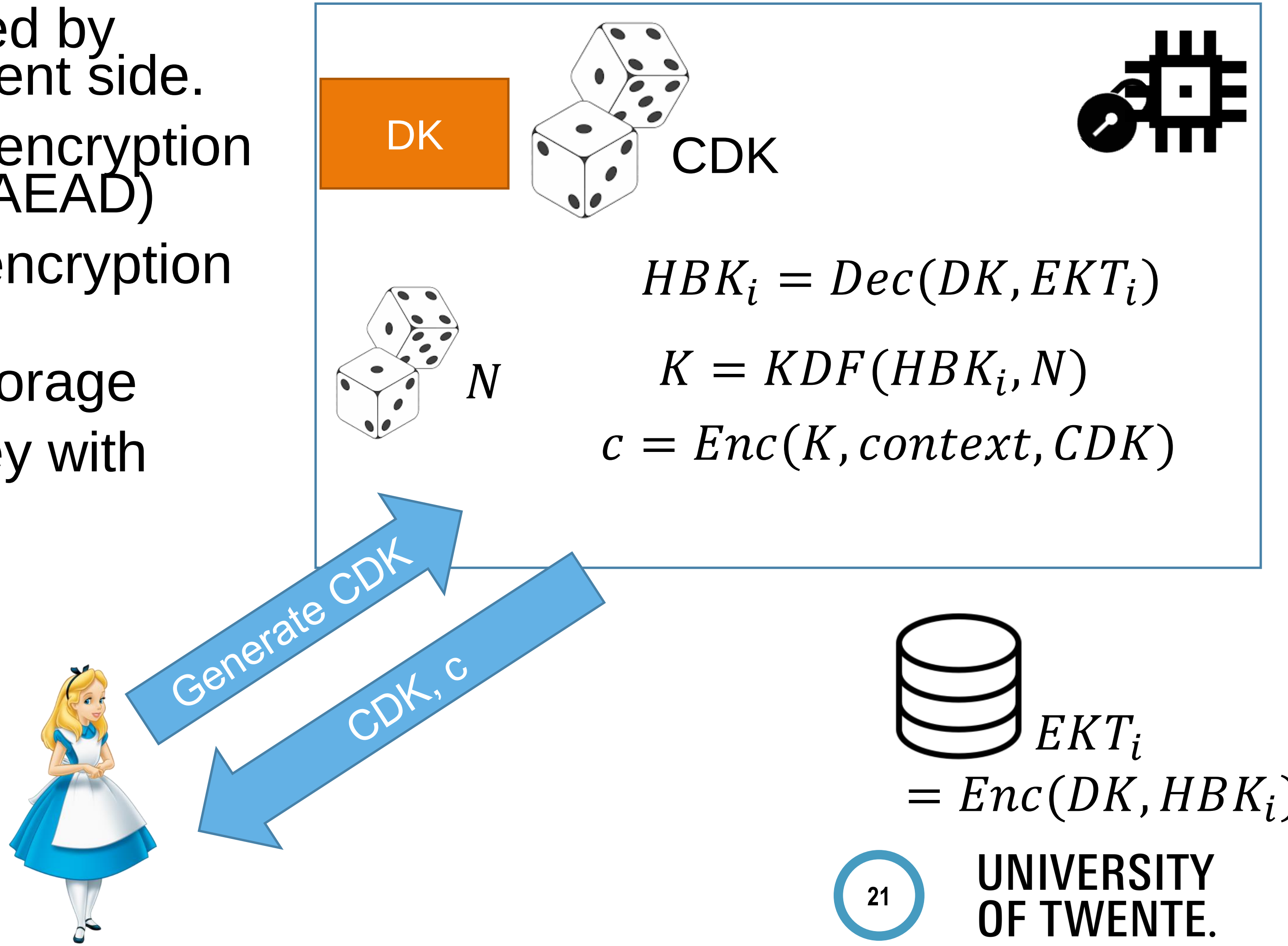
AWS KMS: Customer Data Keys

Customer Data Key can be used by customer to encrypt data on client side.

AES-GCM is an authenticated encryption scheme with associated data (AEAD)

- Authenticated data is called encryption context in KMS

1. Retrieve EKT from cloud storage
2. Generate customer data key with RNG
3. Decrypt EKT
4. Generate random nonce N
5. Derive AES key K from HBK_i & N
6. Encrypt CDK with K and context



$$HBK_i = Dec(DK, EKT_i)$$

$$K = KDF(HBK_i, N)$$

$$c = Enc(K, context, CDK)$$

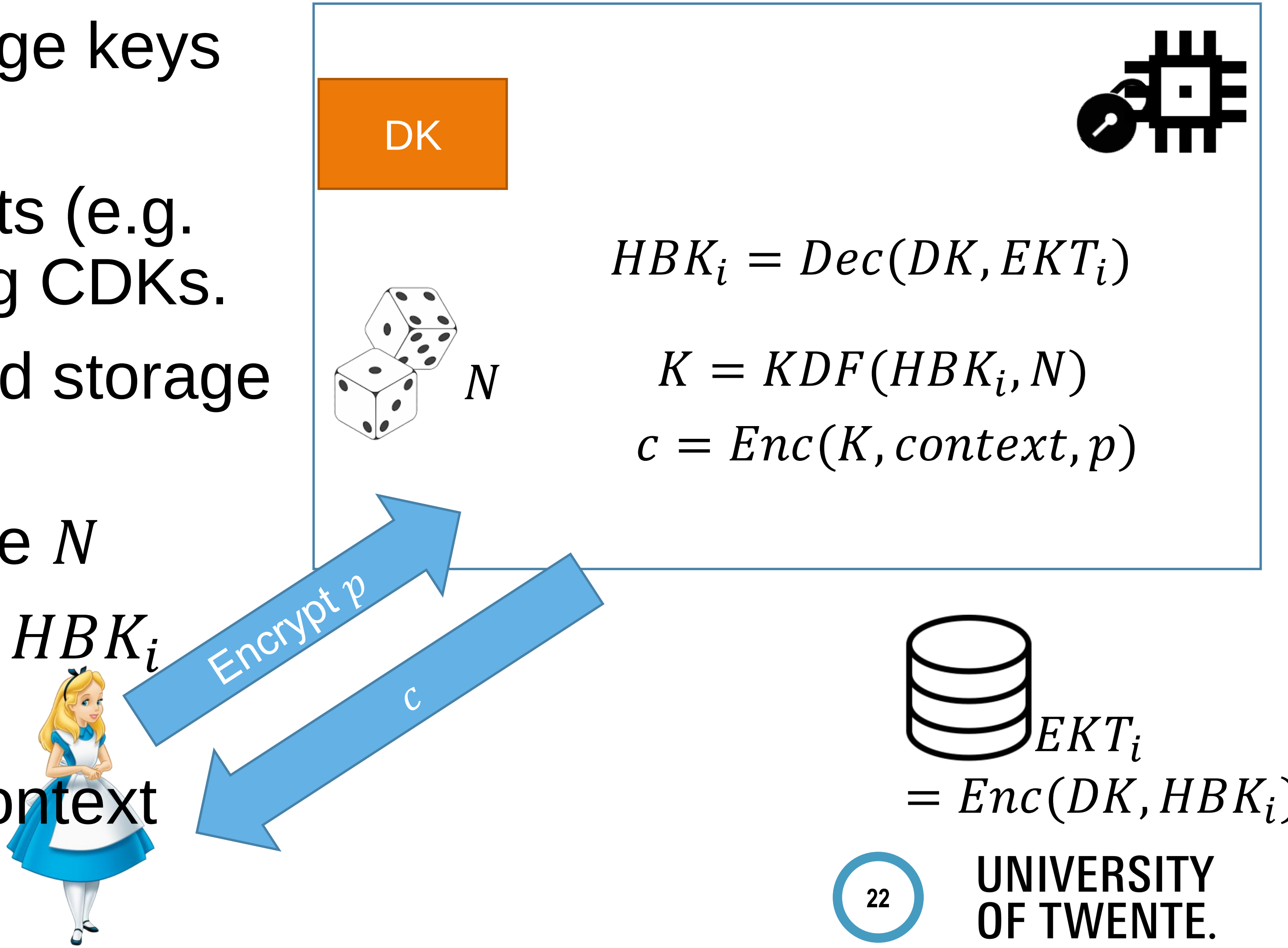
$$EKT_i = Enc(DK, HBK_i$$

AWS KMS: Encryption

KMS is designed for manage keys not using them.

Encryption of 4KB plaintexts (e.g. app keys) is like generating CDKs.

1. Retrieve EKT from cloud storage and decrypt EKT.
2. Generate random nonce N
3. Derive AES key K from HBK_i and N
4. Encrypt p with K and context

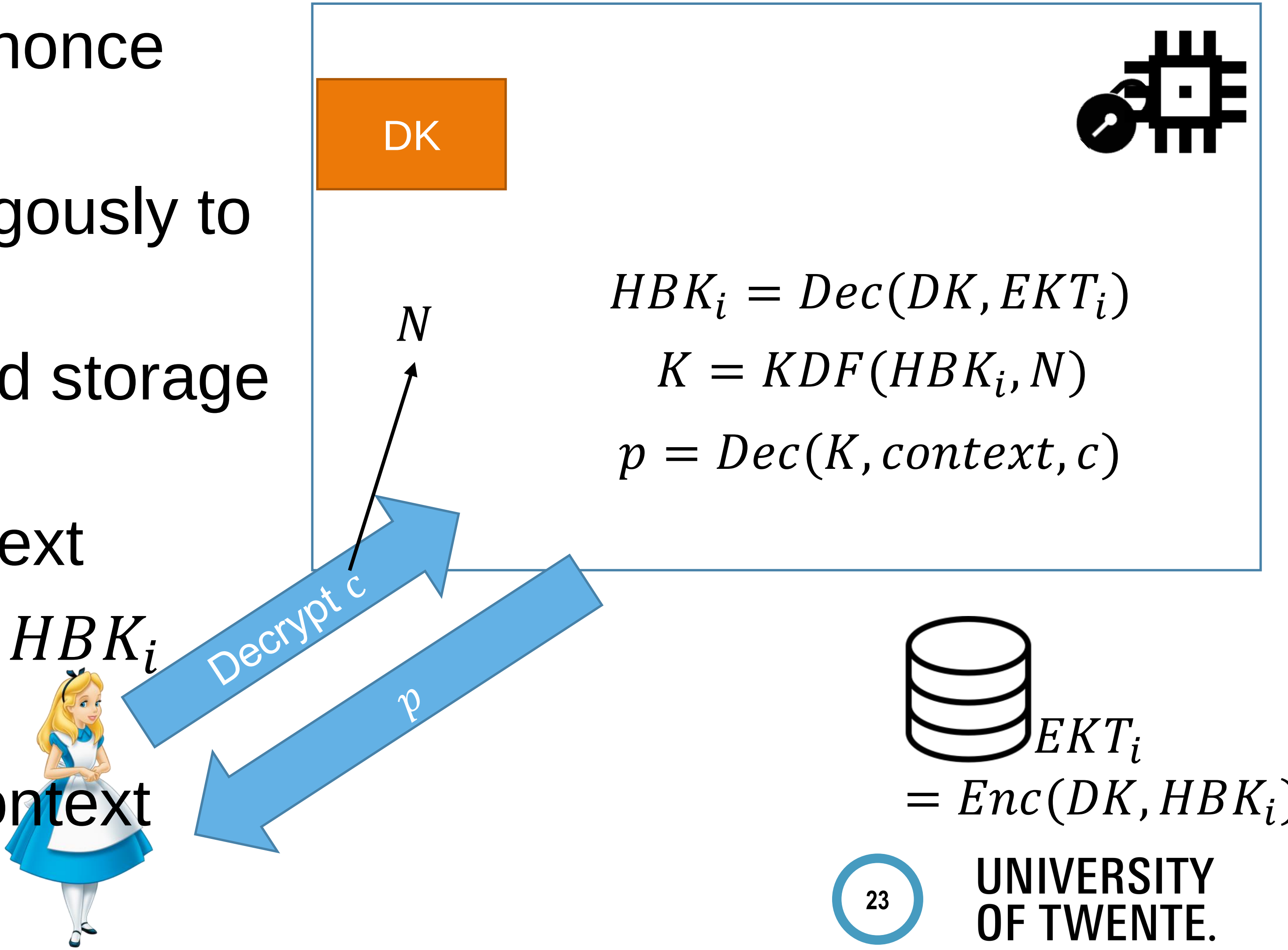


AWS KMS: Decryption

Key is reconstructed from nonce (part of ciphertext)

- Decryption is done analogously to encryption

1. Retrieve EKT from cloud storage and decrypt EKT
2. Retrieve N from ciphertext
3. Derive AES key K from HBK_i and N
4. Decrypt c with K and context



$$HBK_i = Dec(DK, EKT_i)$$

$$K = KDF(HBK_i, N)$$

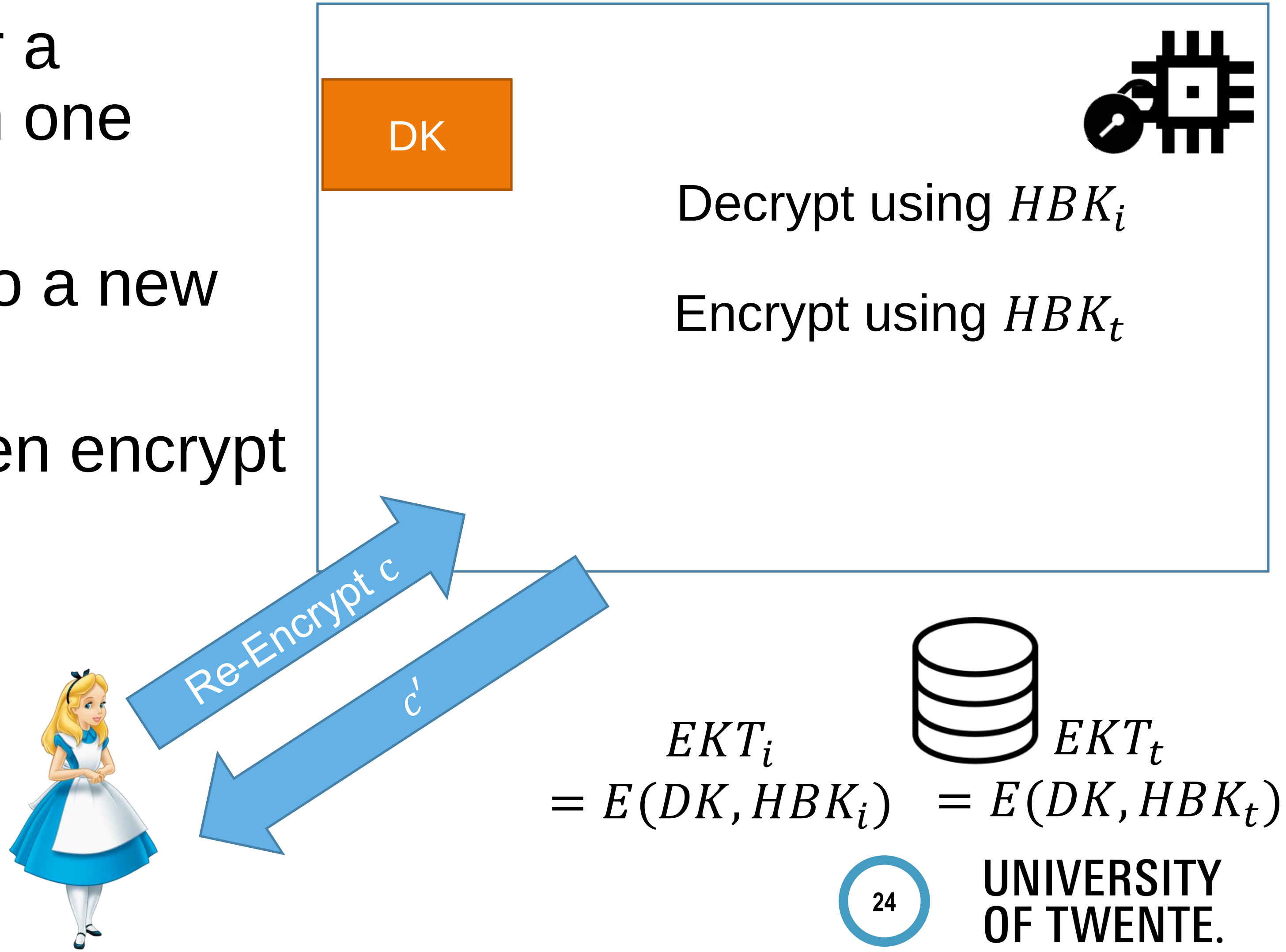
$$p = Dec(K, context, c)$$

AWS KMS: Re-Encryption

Re-Encryption of a CDK or a ciphertext is possible from one CMK to another one

Also, from an old version to a new version for the same CMK

- Decrypt internally and then encrypt again

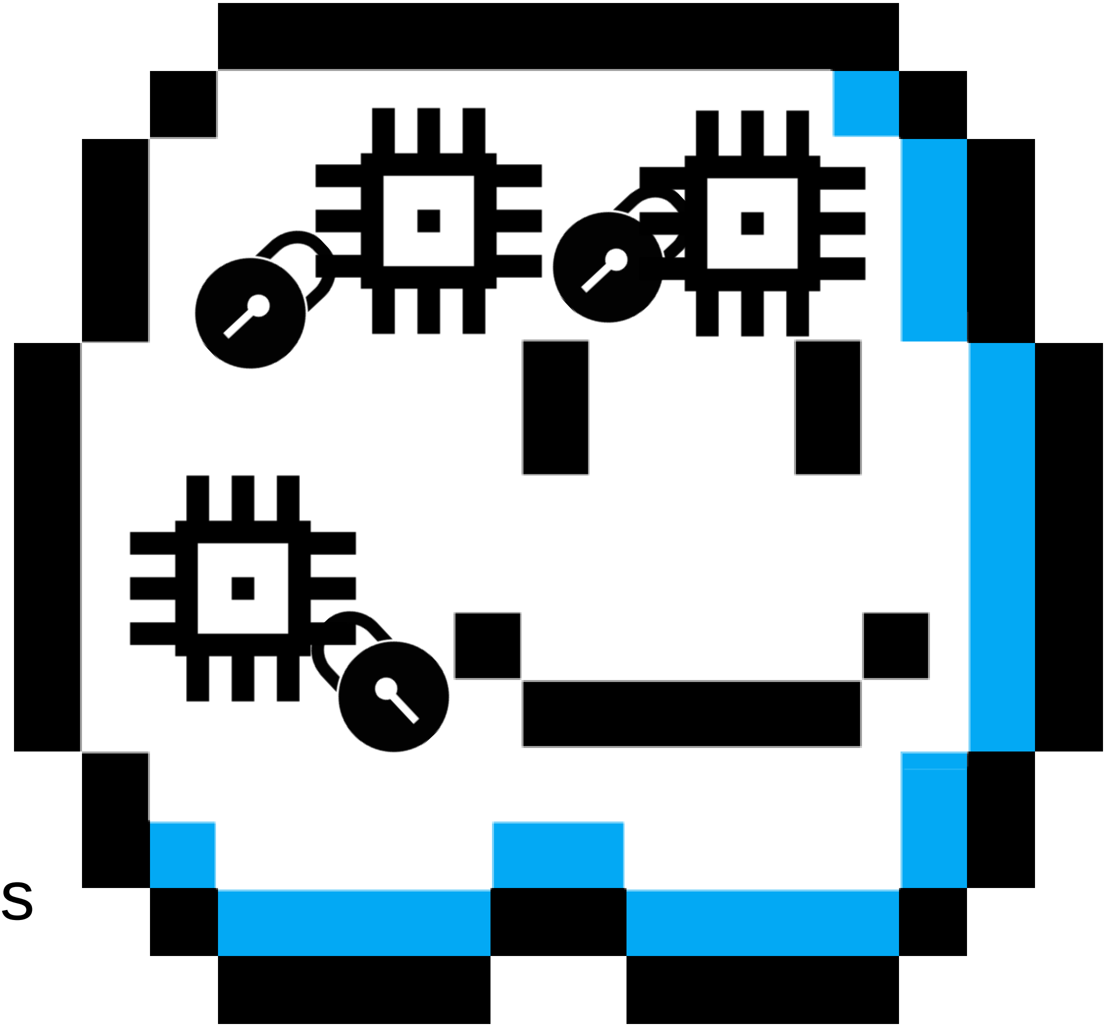


AWS KMS: Domains

Collection of internal AWS KMS entities within one AWS region

Domains have states defined by properties such as:

- Name
- Secret keys (domain keys)
- Members (HSMs) and their public keys
- Operators and their public keys
- Rules



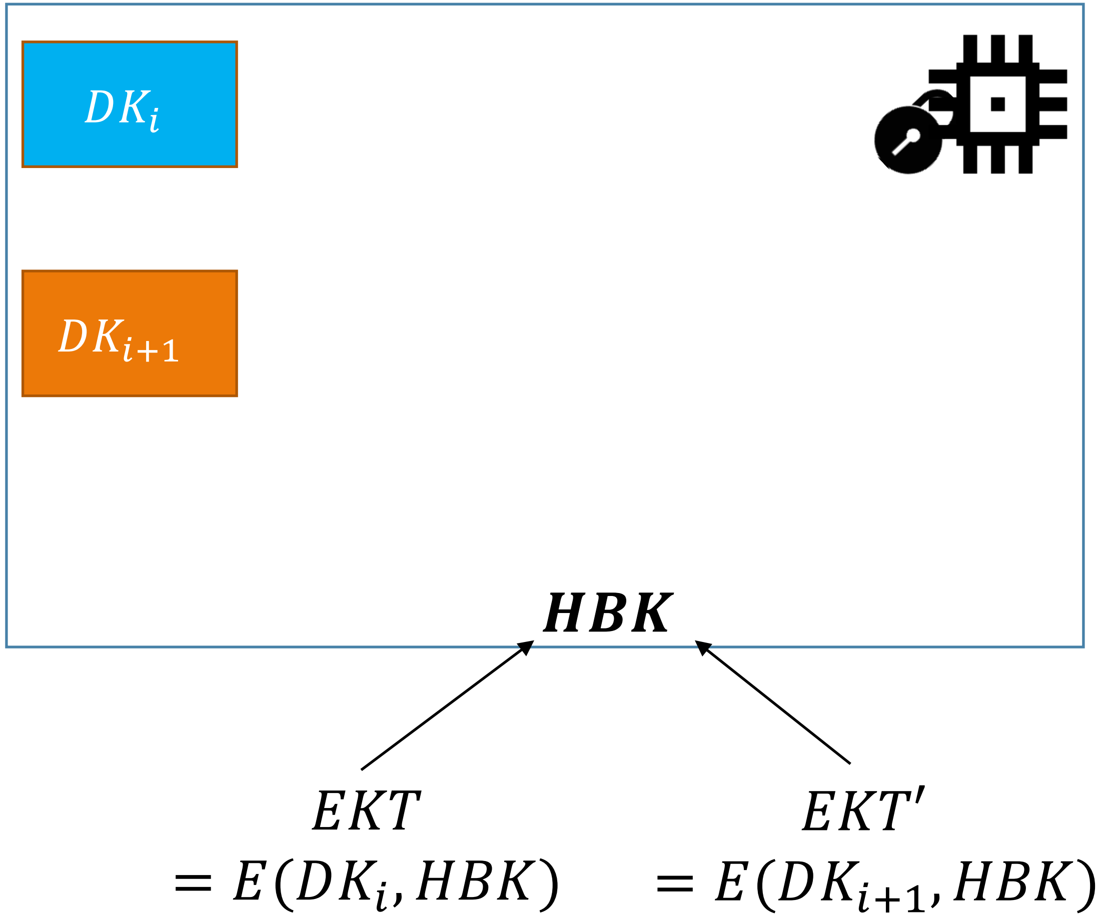
AWS KMS: Domain Keys

Domain keys are set of keys shared by all HSMs

- Used to encrypted HBK before storing externally

Domain keys are rotated on a daily basis by Amazon internally

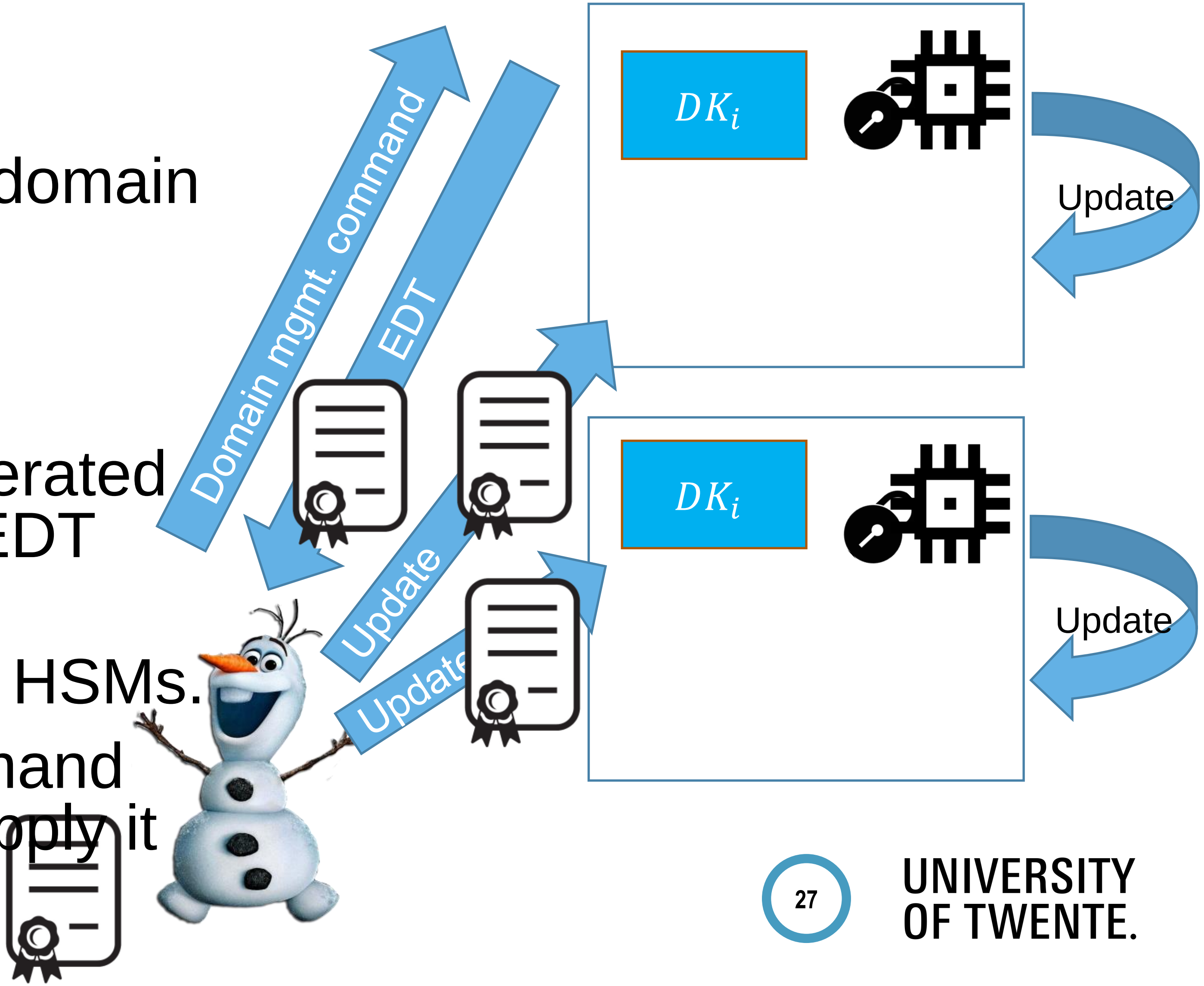
- All EKTs are re-encrypted with new domain key



AWS KMS: Syncing Domain States

For syncing, HSMs do not communicate directly but via operators sending exported domain tokens (EDT)

1. Operator sends domain management command
2. New domain state is generated and exported as signed EDT
3. Operator sends update command with EDT to all HSMs.
4. HSMs authenticate command and domain token then apply it



UNIVERSITY OF TWENTE.

AWS KMS: Rotating Domain Key

Each HSM has two public keys:

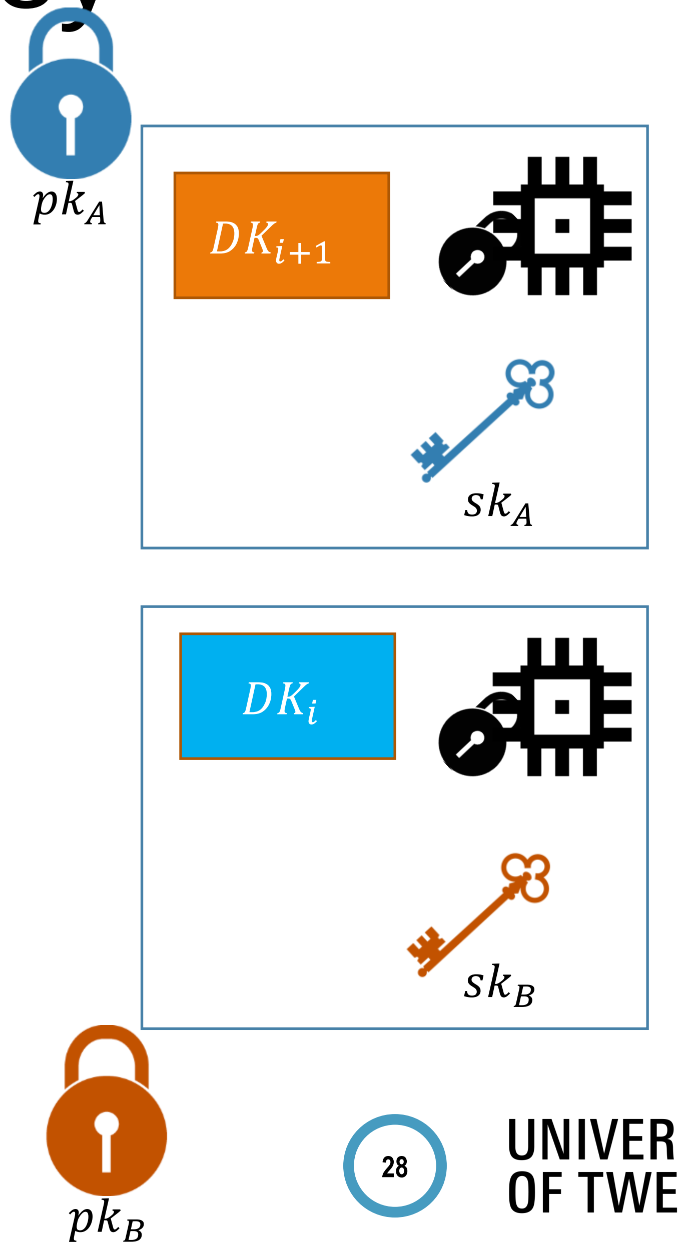
- HSM identity (signature) key pair
- HSM agreement key pair

One HSM generates new domain key and encrypts it

- Encrypts new domain keys with agreement public keys of each HSMs

Sends signed EDT back to operator.

- Operator cannot read DK due to encryption



AWS KMS: DK Encryption Details

Agreement key pair for party P_i is a pair of Diffie-Hellman parameters

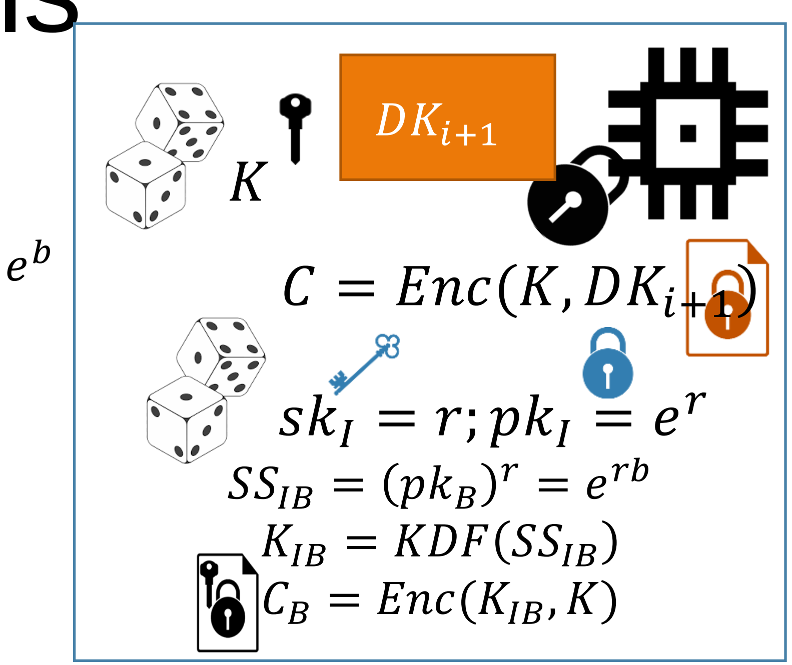
- Public value $pk_{P_i} = e^{p_i}$
- Private value $\mathrm{sk}_{P_i} = \mathrm{p_i}$

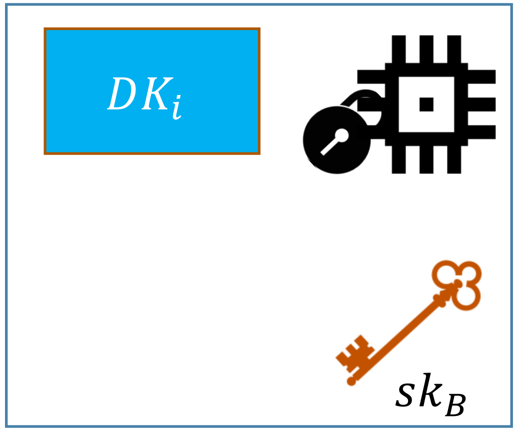
Envelope encryption of domain key DK_{i+1}

- Sample ephemeral secret key K
- Encrypt domain key $Enc(K, DK_{i+1})$
- Sample random DH private value r and DH public value e^r
- For each member P_i:
  - Calculate shared secret $SS_{IP_i} = (e^{p_i})^r$
  - Derive joint key $K_{IP_i} = KDF\left(SS_{IP_i}\right)$
  - Encrypt $C_{P_i} = Enc(K_{IP_i}, K)$

Send $e^r, Enc(K, DK_{i+1}), \{Enc(K_{AP_i}, K)\}$

$pk_B = e^b$





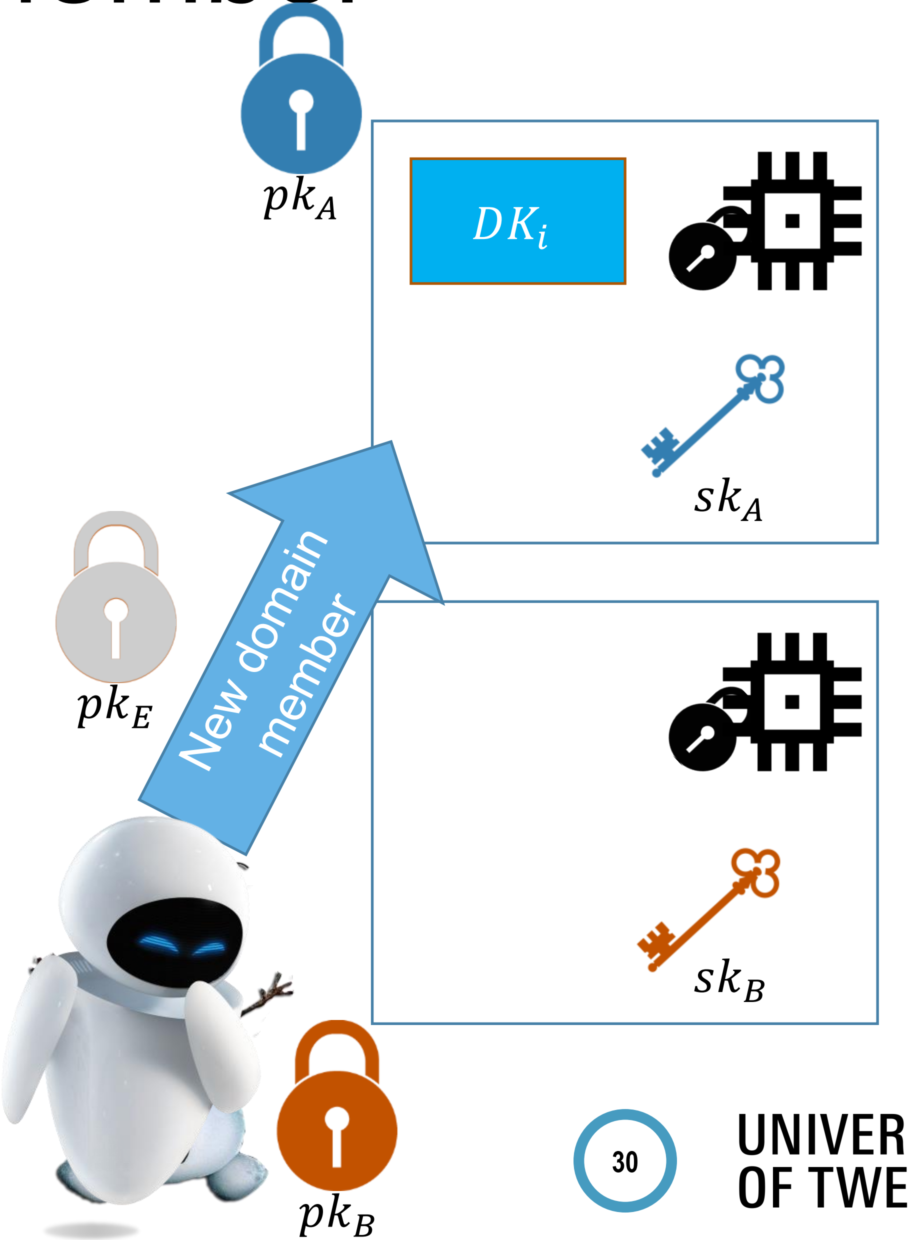
AWS KMS: New Domain Member

Domain HSMs can be synced via exported domain tokens

Join operation executed by operator to add new HSM to domain state:

- Operator updates the domain state including the new public keys
- New keys are synced via syncing protocol

Malicious operator can infiltrate trusted members

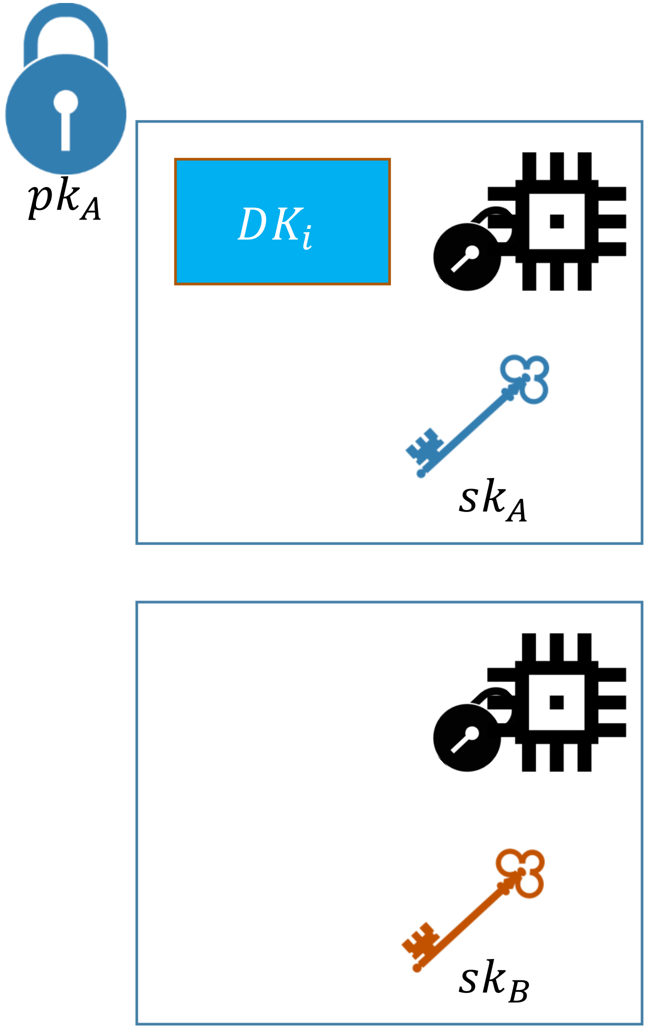


AWS KMS: Consensus

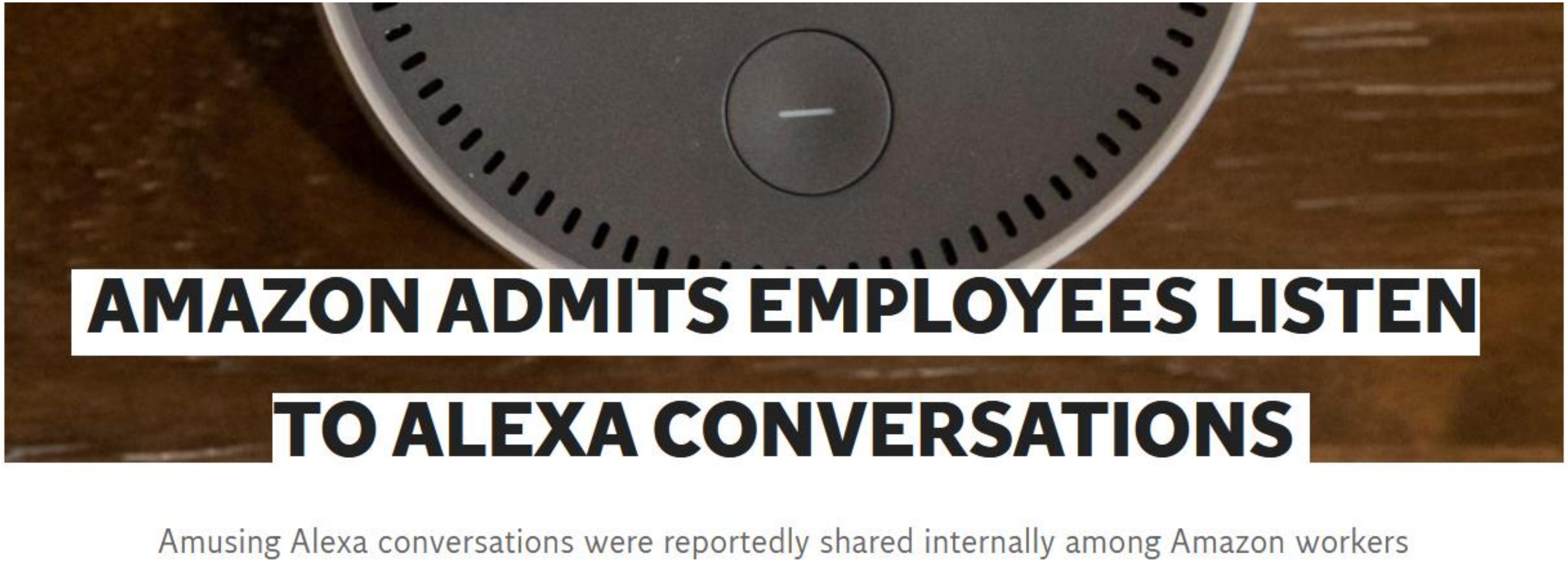
Instead of one operator, multiple operators confirm each operation

- For each operation, a list of quorum rules is defined in domain state
- Digital signature by each operator
- Only commands that fulfill a rule allow domain state changes

Trust Issues solved?



AWS KMS: Conclusion



AMAZON ADMITS EMPLOYEES LISTEN TO ALEXA CONVERSATIONS

Amusing Alexa conversations were reportedly shared internally among Amazon workers

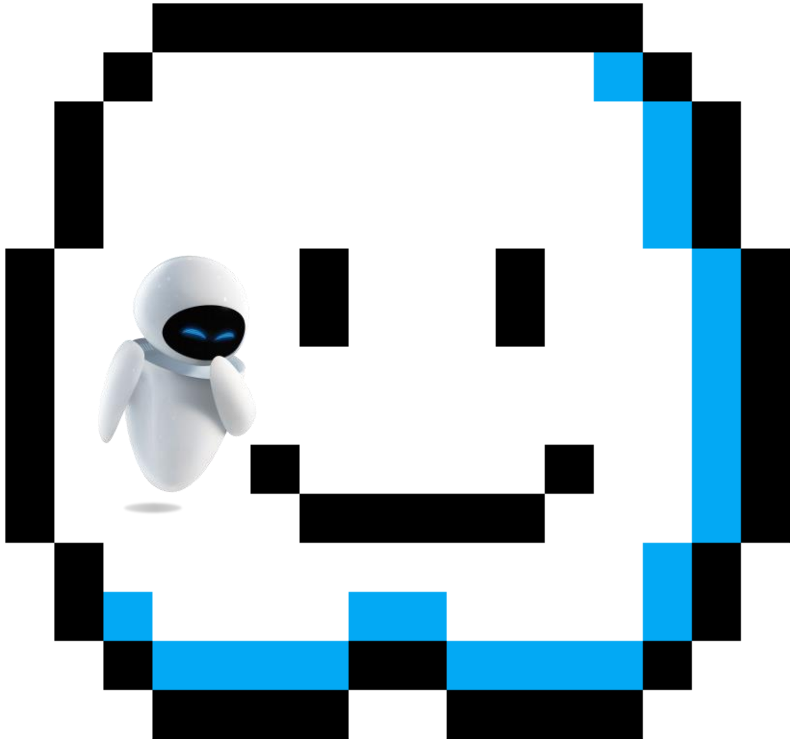
- Trust in A

Amazon spies on staff, fires them by text for not hitting secretive targets, workers 'feel forced to work through pain, injuries' – report

Cloud Security against internal attackers

Integrity

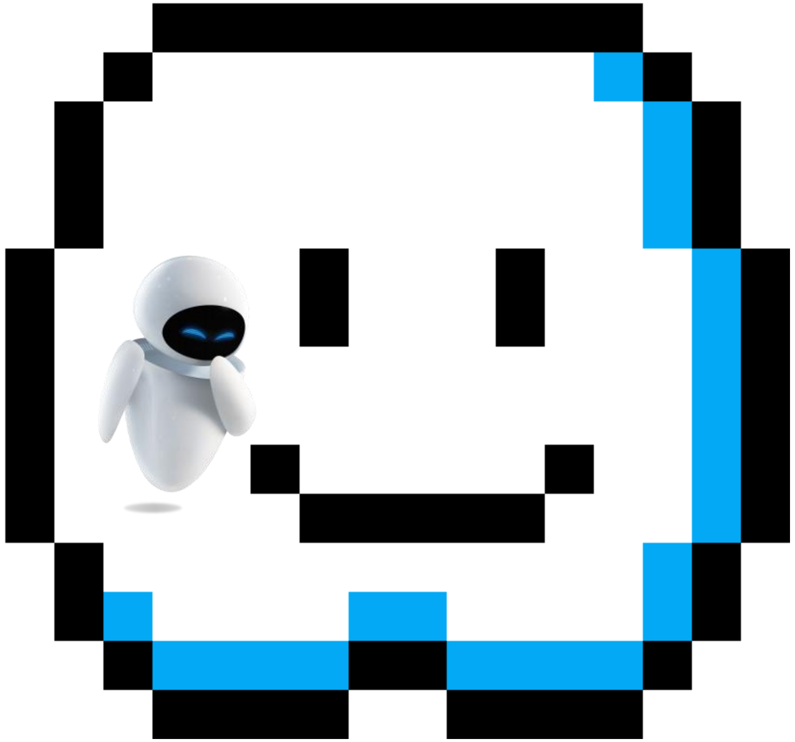
- How do I know that the cloud provider is doing the computations correctly?
- How do I ensure that the cloud provider really stored my data without tampering with it?



Cloud Security against internal attackers

Availability

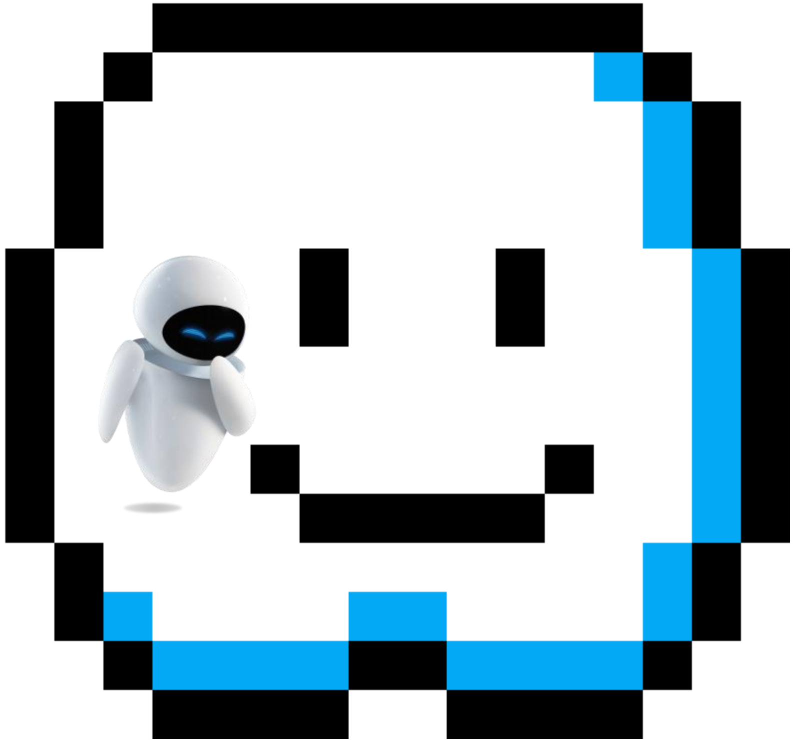
- Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
- What happens if cloud provider goes out of business?



Cloud Security against internal attackers

Privacy issues raised via massive data mining

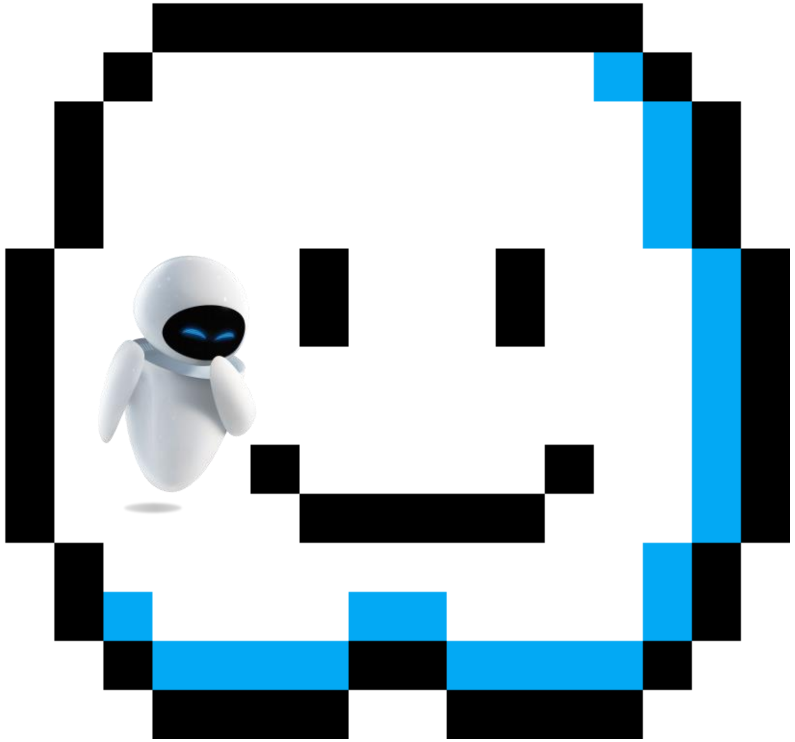
- Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients



Cloud Security against internal attackers

Increased attack surface

- Entity outside the organization now stores and computes data, and so
- Attackers can now target the communication link between cloud provider and client
- Cloud provider employees can be phished

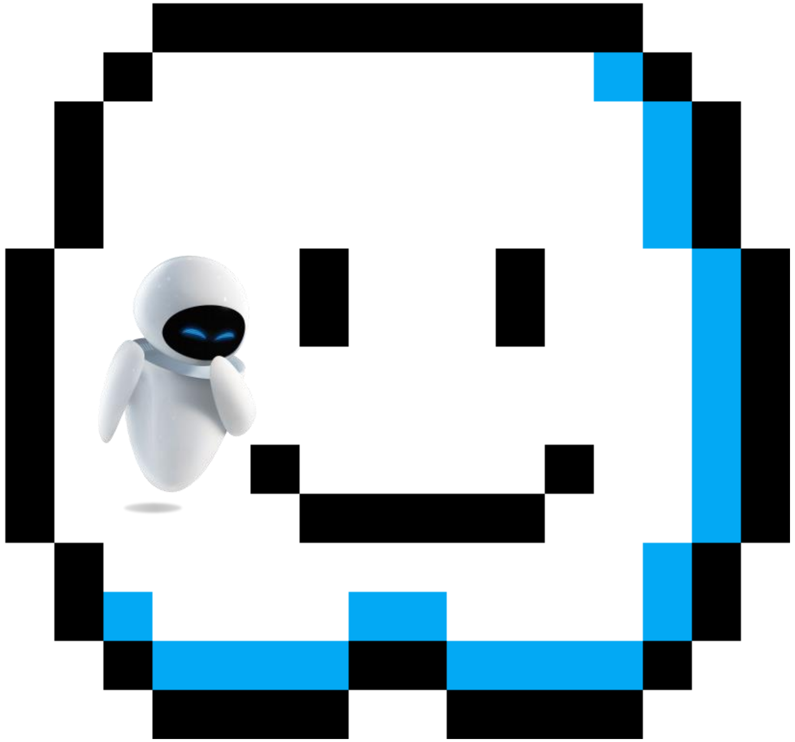


Cloud Security against internal attackers

Auditability and forensics

- Difficult to audit data held outside organization in a cloud

- Forensics are more difficult for clients since they don’t maintain data locally

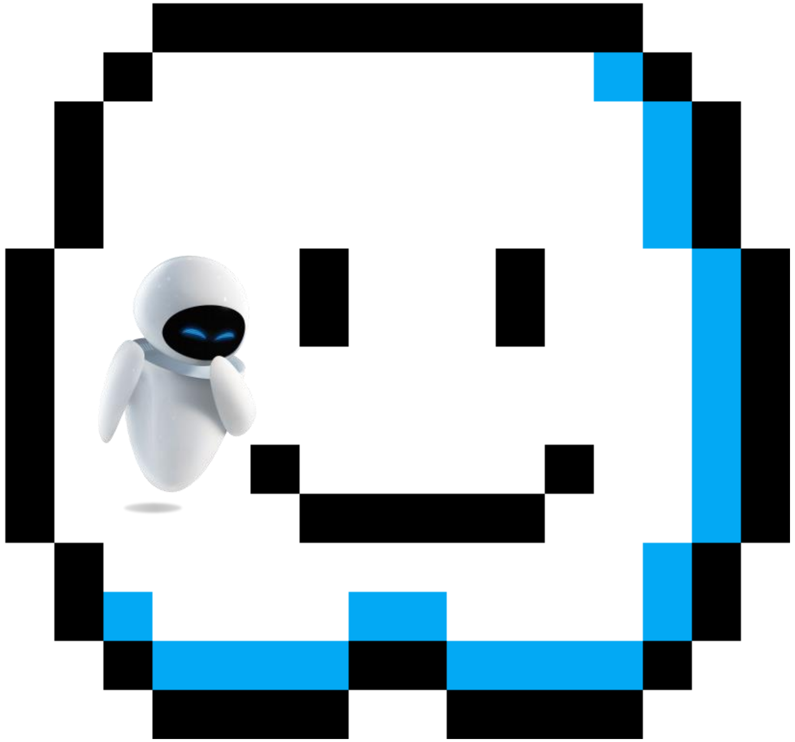


Cloud Security against internal attackers

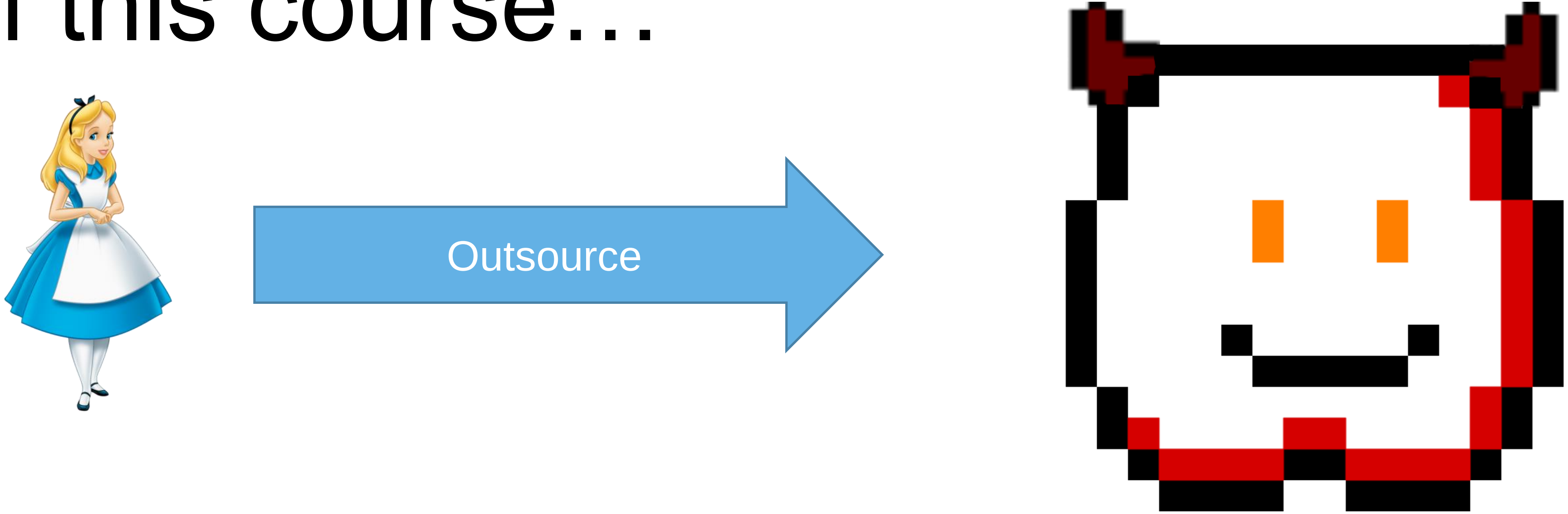
Confidentiality

- Will the sensitive data stored on a cloud remain confidential? Will cloud compromises leak confidential client data (i.e., fear of loss of control over data)

- Will the cloud provider itself be honest and won't peek into the data?



Focus of this course…



Cryptographic protection against semi-honest (honest-but-curious) clouds:

- Cloud provider follows protocol and does not deviate from it (risk of getting caught)
- Different scenarios, protection goals and cryptographic tools
- Discuss different aspects: performance analysis, security proofs, use-cases and limitations

Excursion into cloud security in the real world from end-user perspective

Questions