Welcome to CompTIA Security+ Day One

Michael J. Shannon
CISSP, CCSP, CCSK,
ITIL 4 Managing Professional

Class will begin at 10:00 am
Central Standard Time

SECURITY GOALS AND CONTROLS

Objectives

- Provide an overview of confidentiality, integrity, availability, and non-repudiation
- Describe the concepts of authentication, authorization, and accounting (AAA)
- Describe control categories
- Define control types

THE CIA TRIAD

CONFIDENTIALITY

AVAILABILITY

INTEGRITY

CONFIDENTIALITY

- Measures an attacker's ability to get unauthorized access to data or information from an application or system
- Involves using techniques, often cryptography, to allow only approved subjects with the ability to view information
- Includes preserving authorized restrictions on information access and disclosure

CONFIDENTIALITY

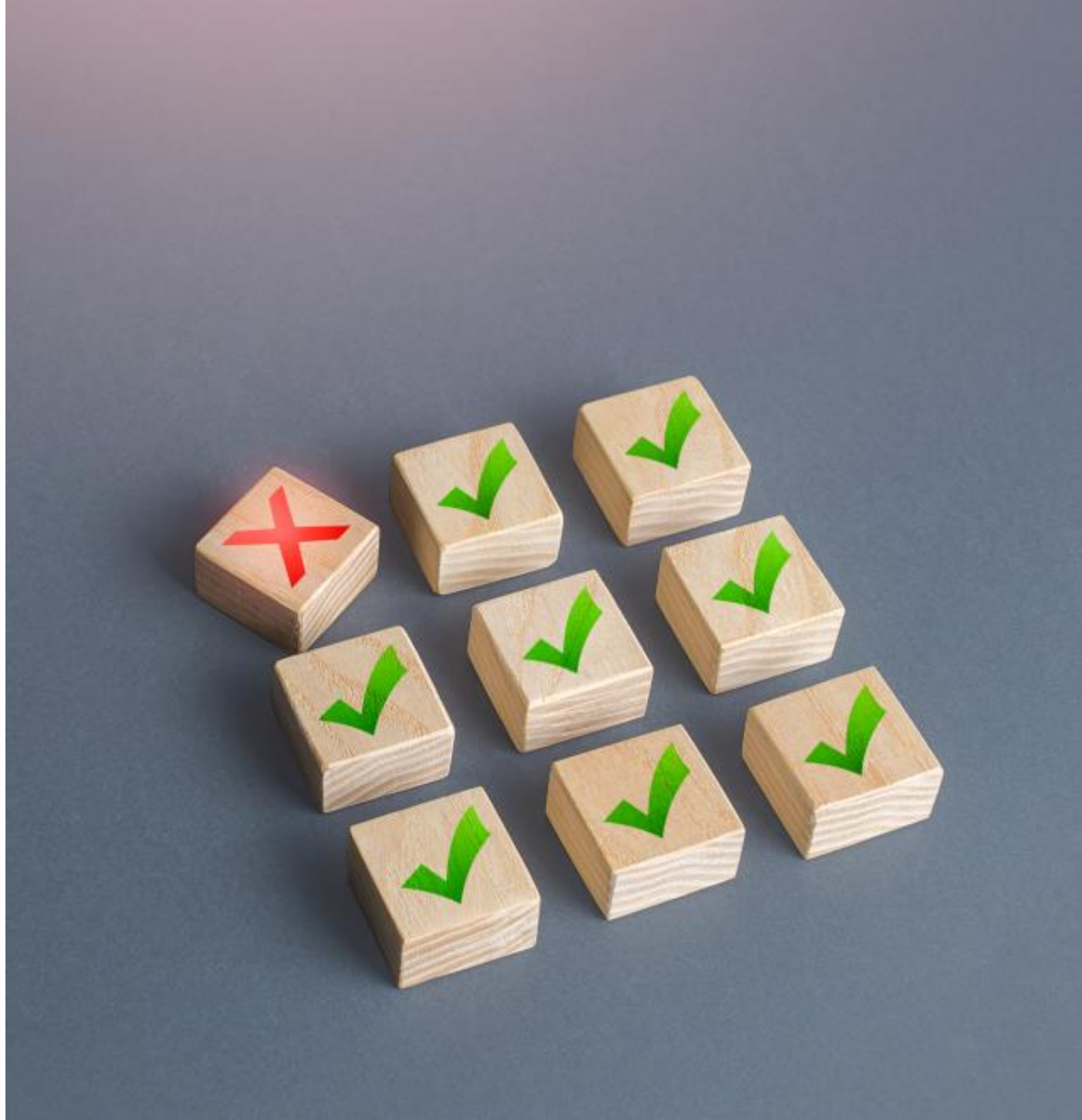
- It is a means for protecting personal privacy and proprietary information
- Confidential information can include passwords, cryptographic keys, personally identifiable information (PII), personal health information (PHI), intellectual property (IP), or other sensitive information

EXAMPLES OF CONFIDENTIALITY

- Using an IPsec virtual private network (VPN)
- Leveraging mutual Transport Layer Security (TLS) between a web browser and web server or controller
- Storing sensitive data or credentials in a mobile device partition or secure enclave
- Implementing Advanced Encryption Standard (AES) encryption on data at rest in storage (file, block, object, databases, etc.)

INTEGRITY

- Involves safeguarding against improper information modification or destruction
- Is a property that data or information have not been altered or damaged in an unauthorized way
- Is the quality of an IT system that reflects:
  - The logical correctness and reliability of the operating system
  - The logical completeness of the hardware and software that implements the protection mechanisms
  - The consistency of the data structures and occurrence of the stored data

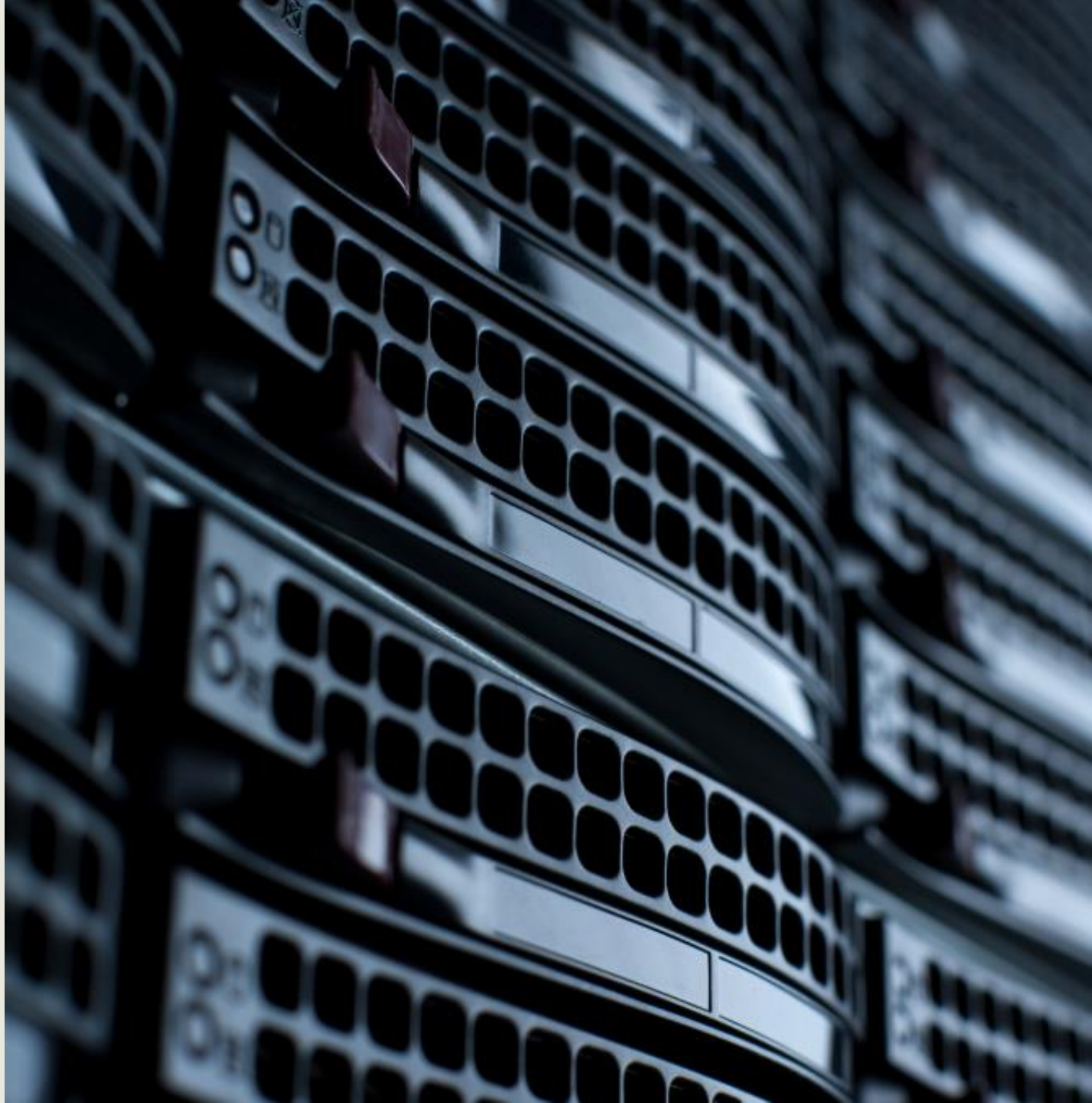


EXAMPLES OF INTEGRITY

- An operating system that performs a mathematical checksum when a file is moved or copied from one volume to another
- A frame check sequence conducted on an Ethernet frame when sent from one MAC address to another
- A hashed message authentication code applied to advertisements sent between neighbor systems such as routers or gateways
- Implementation of a mandatory access model technique such as Biba or Clark-Wilson

AVAILABILITY

- Availability is the process of ensuring timely and reliable access to and use of information
- It is a property of data, information, applications, systems, or services that are accessible and usable upon demand by an authorized subject
- "High availability" is a failover feature to ensure availability during device or component interruptions both, planned and unplanned



EXAMPLES OF AVAILABILITY

- Implementing security controls that protect systems and services from spoofing, flooding, denial-of-service (DDoS), poisoning, and other attacks that negatively affect the ability to deliver data, content, or services:
  - Vulnerabilities that impact availability can affect hardware, software, and network resources, such as flooding network bandwidth, consuming large amounts of memory, CPU cycles, or unnecessary power consumption

EXAMPLES OF AVAILABILITY

- Assuring that technical controls such as firewalls, intrusion prevention system (IPS) sensors, anti-virus, and endpoint protection are always reliable and deployed in a failover group or cluster
- Determining the best disaster recovery site solution for every scenario or situation for an organization

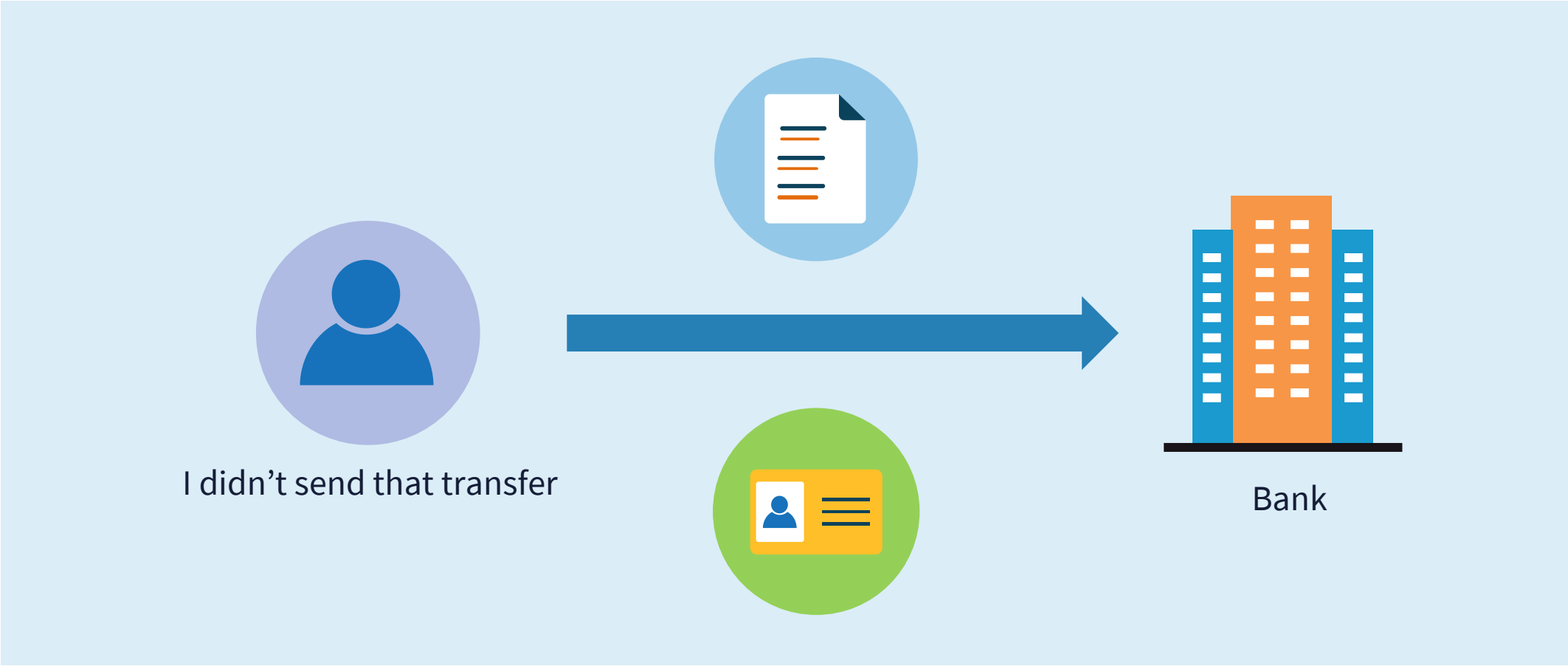
NON-REPUDIATION

- Non-repudiation refers to enforcing the inability of a subject to deny that they participated in a digital transaction, agreement, contract, or communication such as an email
- Non-repudiation is the property of agreeing to adhere to an obligation:
  - More specifically, it is the inability to refute responsibility

NON-REPUDIATION

- For example, if you take a pen and sign a (legal) contract, your signature is a non-repudiation device
- In IT, non-repudiation is usually accomplished with a public/private key pair cryptosystem and digitally signed certificates between the sending and receiving parties

REPUDIATION OF ORIGIN



AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA)

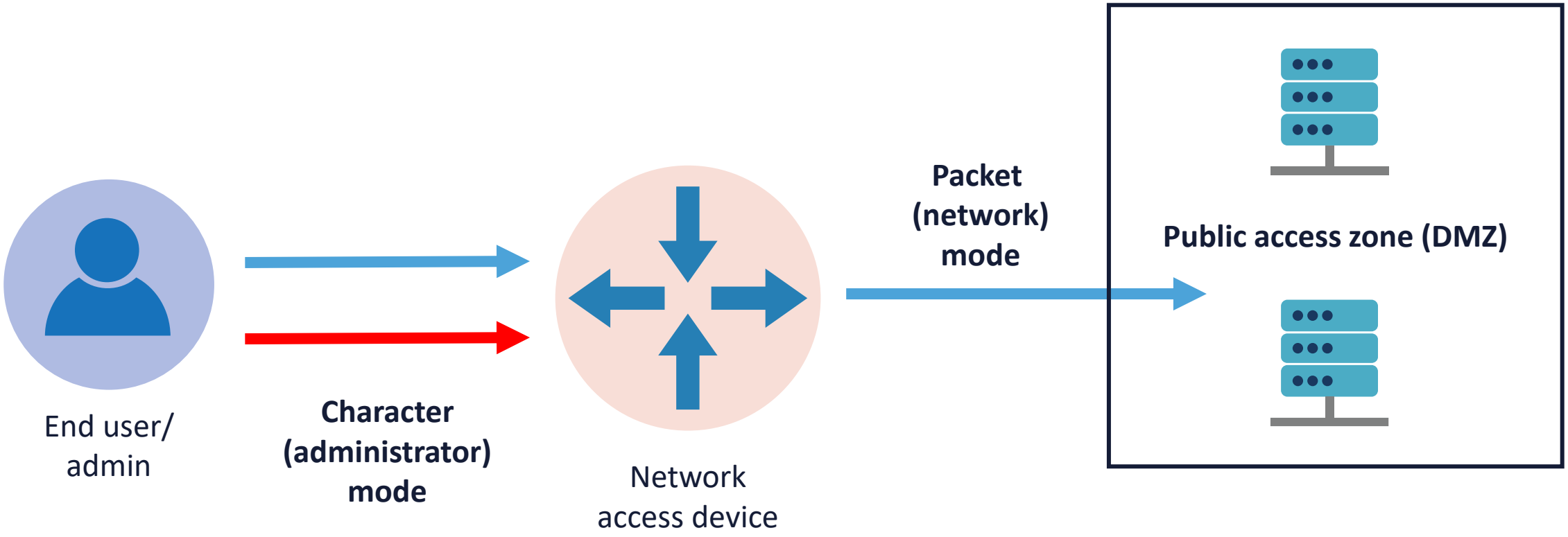
- **Authentication** – the process of validating that an entity (user, application, or system) is who or what they claim to be
- **Authorization** – the process of granting an authenticated entity permission to access a resource or perform a specific function
- **Accounting** – basically, when did the entity begin, when did it end, and how long did they do it?

CHARACTER MODE VS. PACKET MODE

Character mode sends keystrokes and commands (characters) to a network admission device for the purpose of configuration or administration on THAT same device

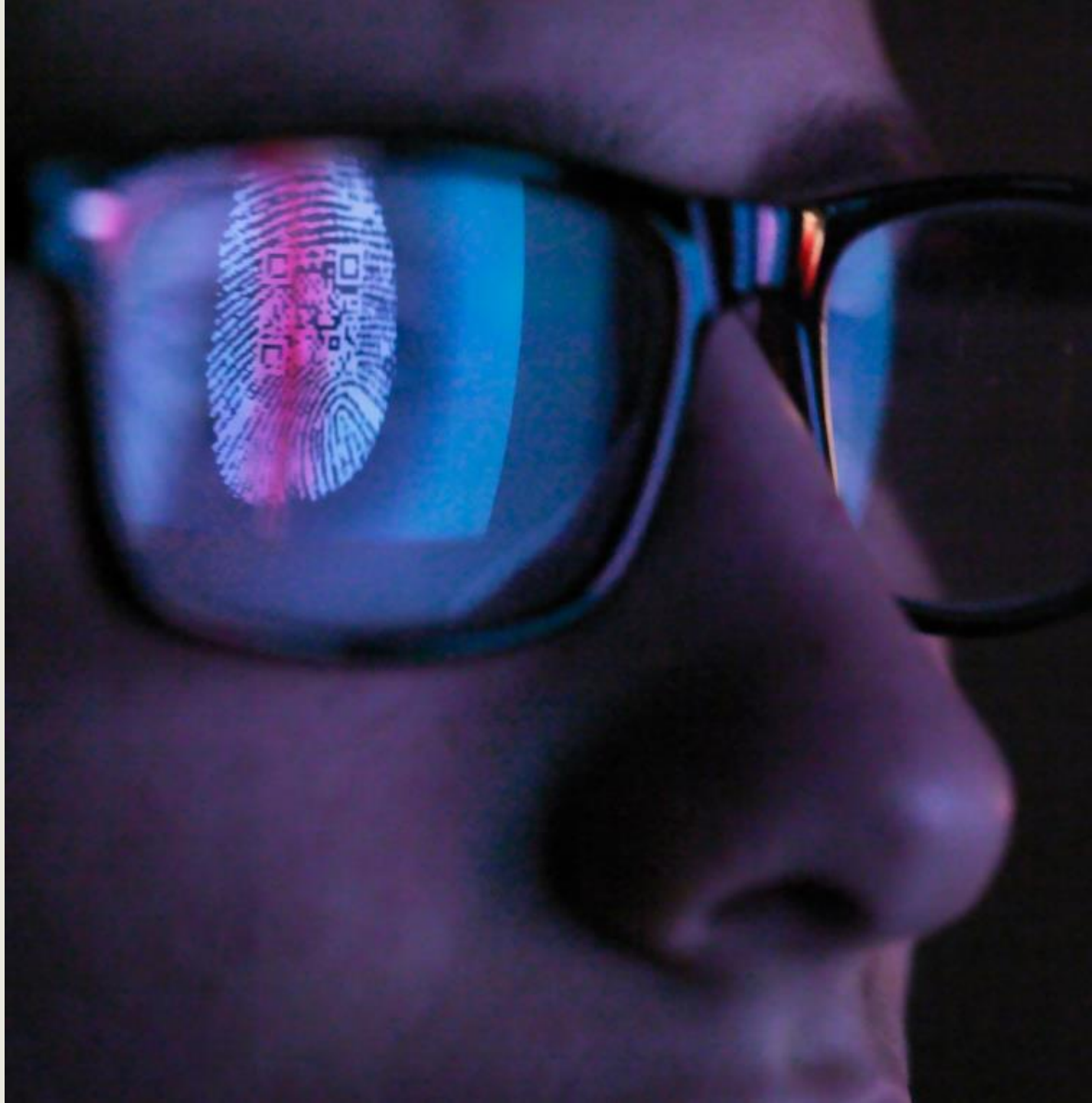
Packet (or network) mode occurs when the network admission device serves as an authentication proxy on behalf of services in other networks such as the web, File Transfer Protocol (FTP), domain name system (DNS), etc.

CHARACTER VS. PACKET MODE



AUTHENTICATION

- Authenticating subjects is technically mandatory, even if using open or anonymous techniques
- Historically, clients would initiate a Transmission Control Protocol (TCP) three-way communication handshake before the authentication process
- This is now considered sub-optimal and a violation of "zero trust" principles



AUTHORIZATION

- Authorization is technically optional for authenticated entities and is mandatory from a practical policy standpoint
- In modern security deployments, it is desirable to implement session-based (tokens) and attribute-based authorization mechanisms

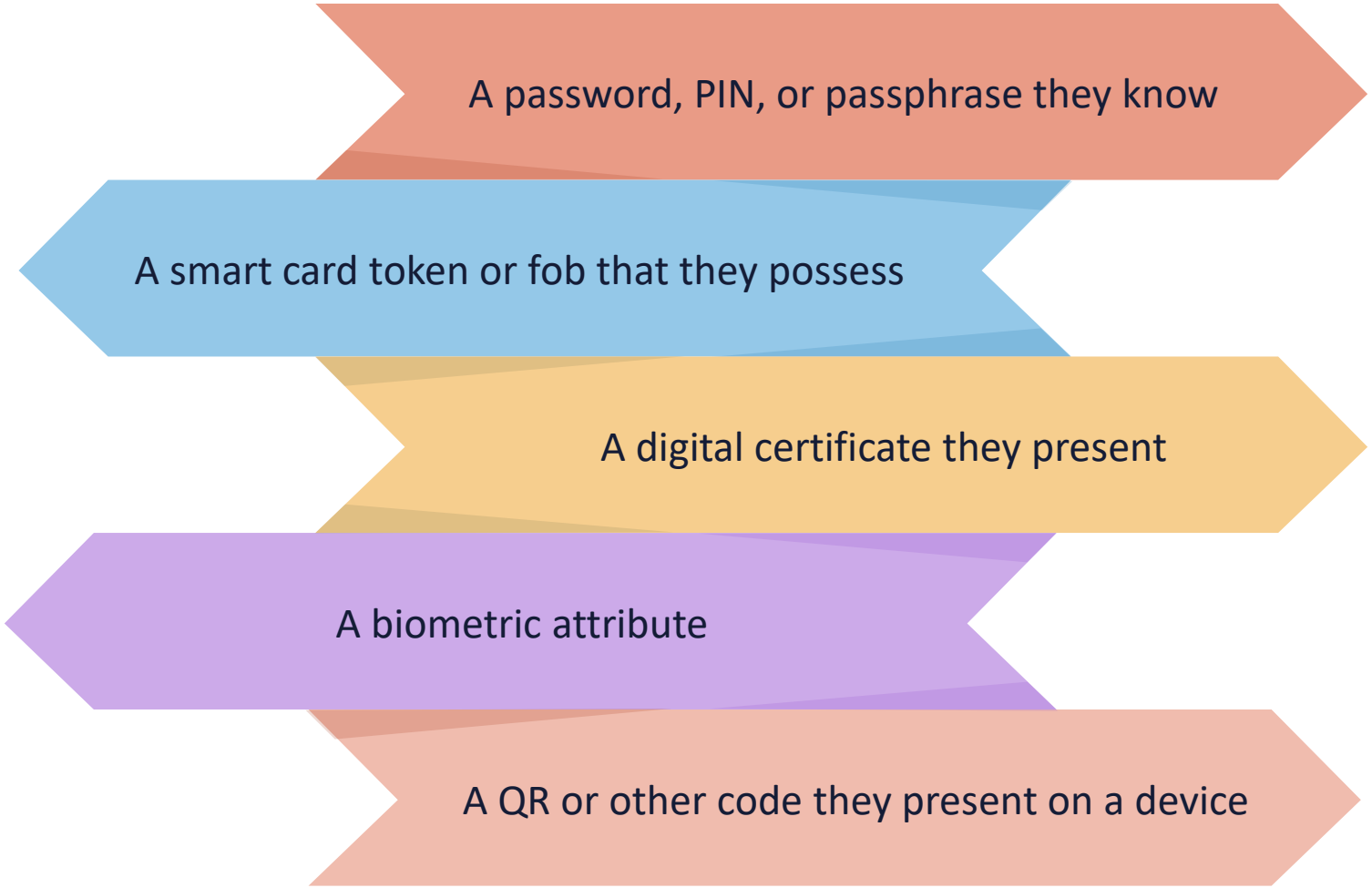
ACCOUNTING

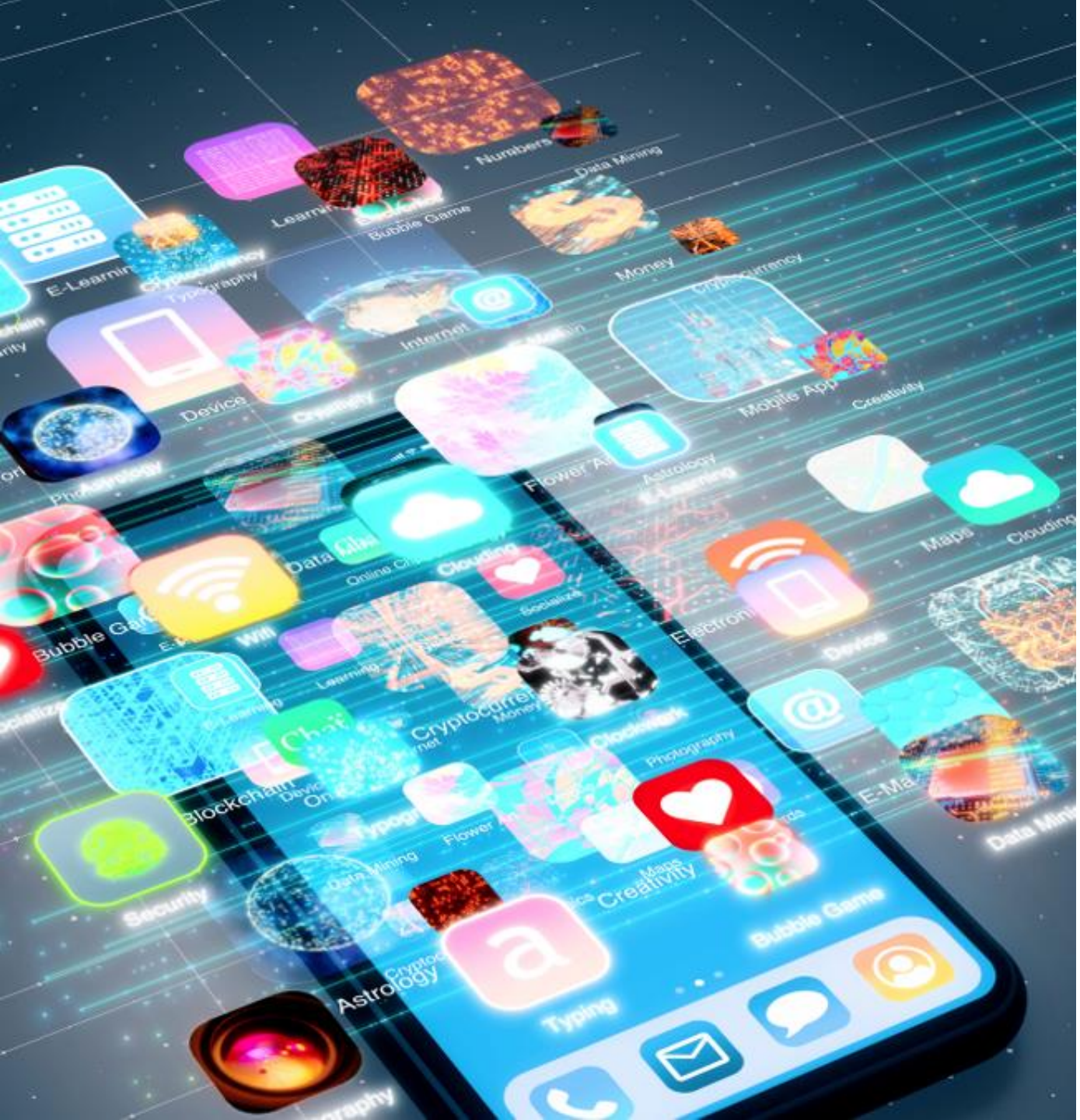
- Accounting is generally implemented for two use cases:
  - Monitoring, visibility, and reporting
  - Billing, chargeback, and reporting
- Remote Authentication Dial-in User Service (RADIUS) is one of the most popular Internet Engineering Task Force (IETF)-based AAA services, and it is known for exceptional accounting capabilities
- Diameter is the next generation of RADIUS

AUTHENTICATING PEOPLE

- Authenticating a person entity means confirming that they are who they claim to be
- This confirms only those with authorized credentials gain access to secure systems
- Usernames/webmail/email and a password is still the most common factor for authenticating people
- There should always be another robust factor added to a simple credential today

COMMON WAYS TO AUTHENTICATE PEOPLE





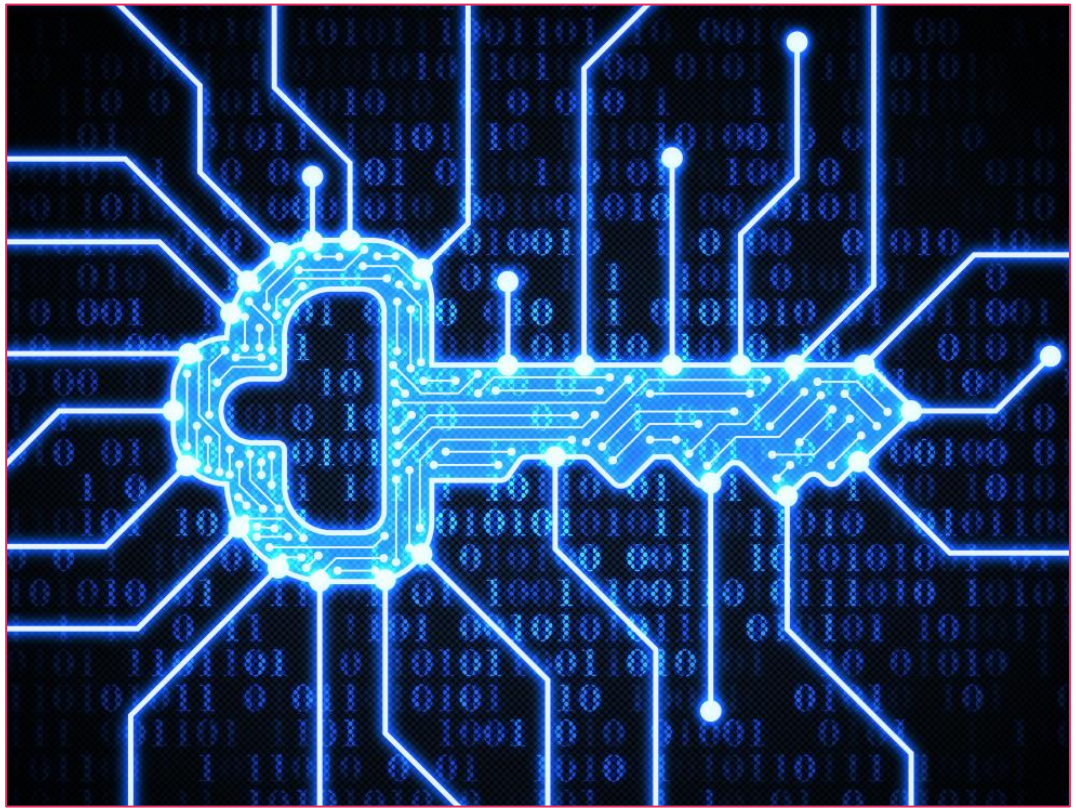
AUTHENTICATING DEVICES AND SYSTEMS

- There are many different types of entities or principals that can be authenticated other than people
- These subjects are often called "non-person entities" (NPEs):
  - Laptops and pads
  - Mobile devices
  - Gateways and load balancers
  - Robotics systems
  - Embedded devices
  - Internet of Things (IoT) endpoints

ENDPOINT AUTHENTICATION

- Endpoint (or device) authentication is a security technique designed to ensure that only authorized devices can connect to a given network, site, or service
- Endpoint security management is rapidly emerging as an important area in machine-to-machine (M2M) communications and IoT
- **Endpoint fingerprinting** is one way to enable authentication of non-traditional network endpoints such as smart card readers, HVAC systems, medical equipment, and IP-enabled door locks

COMMON DEVICE (ENDPOINT) AUTHENTICATION METHODS



- A shared secret key stored on endpoints (wireless) or infrastructure devices
- An X.509 v3 device certificate stored in a software application
- A cryptographic key, certificate, or other credential stored at the hardware level in a trusted platform module
- A key stored in a hardware security module (HSM)
- A protected access file (PAC) in a Cisco infrastructure

AUTHORIZATION MODELS: DAC

- Discretionary access control (DAC) grants access control decisions to the resource owners and custodians
- Each resource typically has an owner who determines the access permissions and shares
- The owner can grant or revoke access rights for other users or groups
- DAC offers flexibility and allows resource owners to have fine-grained control over access, but it can also result in inconsistent access control decisions
- It is the most prone to "privilege creep"

AUTHORIZATION MODELS: RBAC

- Role-based access control (RBAC) grants access based on predefined roles or job titles
- Users are assigned roles, and access rights are associated with these roles
- Instead of directly assigning permissions to individual users, permissions are assigned to roles, and users inherit the access rights associated with their assigned roles, for example:
  - Various roles in a hospital or medical center
  - Built-in roles in a database management system
- RBAC streamlines access control administration by grouping users with similar job functions and offering a scalable approach to access management

AUTHORIZATION MODELS: MAC

- A mandatory access control (MAC) is a strict mathematical model where access to resources is determined by the system based on predefined security labels and rules
- Principals are assigned security clearances or classification levels (top secret, secret, confidential, etc.)
- Resource objects are labeled with sensitivity levels
- Access is granted or denied by comparing these labels and rules, ensuring strict control and preventing unauthorized access
- This is a "non-discretionary" model

AUTHORIZATION MODELS: ABAC

- Attribute-based access control (ABAC) grants access based on a combination of characteristics associated with users, resources, and environmental conditions
- Attributes can include user attributes (job title, department), resource attributes (sensitivity level, classification), and environmental attributes (time of access, location)
- Authorization policies are defined using these combinations, and decisions are made based on evaluating the attributes against the defined policies

AUTHORIZATION MODELS: ABDAC

- Attribute-based dynamic access control (ABDAC) combines the principles of attribute-based access control (ABAC) with dynamic access control (DAC)
- It considers dynamic factors such as risk assessment, user attributes, resource attributes, and contextual information to make access control decisions in real time
- ABDAC provides more fine-grained and context-aware access control needed in "zero trust" environments when compared to traditional static access control models:
  - May include dynamic machine learning techniques such as user behavioral analytics (UBA) in next-generation environments

AUTHORIZATION MODELS: RULE-BASED

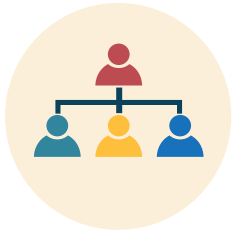
- Rule-based access control (RBAC) uses rules to determine access
- Access control rules define conditions or criteria that must be met for access to be granted
- These rules can be based on several factors, such as user attributes, resource attributes, time of access, and more
- **Access decisions are made by comparing these rules against the context of the access request – usually IP transport and network layer header metadata**

RULE-BASED ACCESS CONTROL LISTS

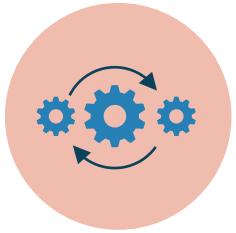
Protocol	Port	Source	Destination	Name	Action
UDP	53	Any	192.16.10.200	Allow DNS queries	Allow
TCP	80,443	Any	192.168.10.201	Allow HTTP and HTTPS	Allow
TCP	3,389	IT_Admin_IP_Range	Any	Allow RDP	Allow
Any	Any	Any	Any	Default	Deny

SECURITY CONTROL CATEGORIES

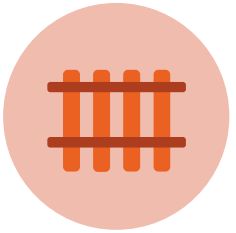
Technical



Managerial



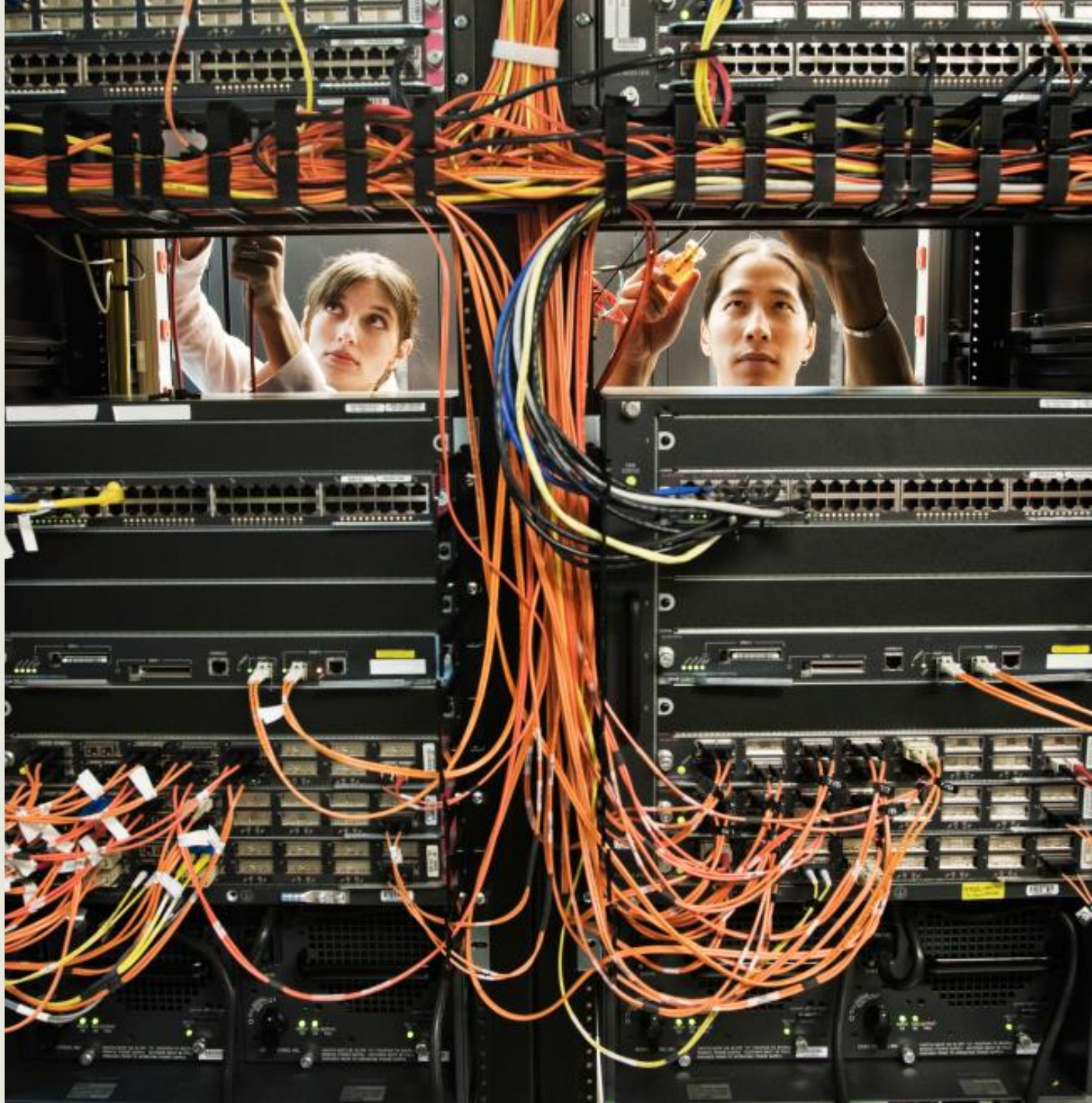
Operational



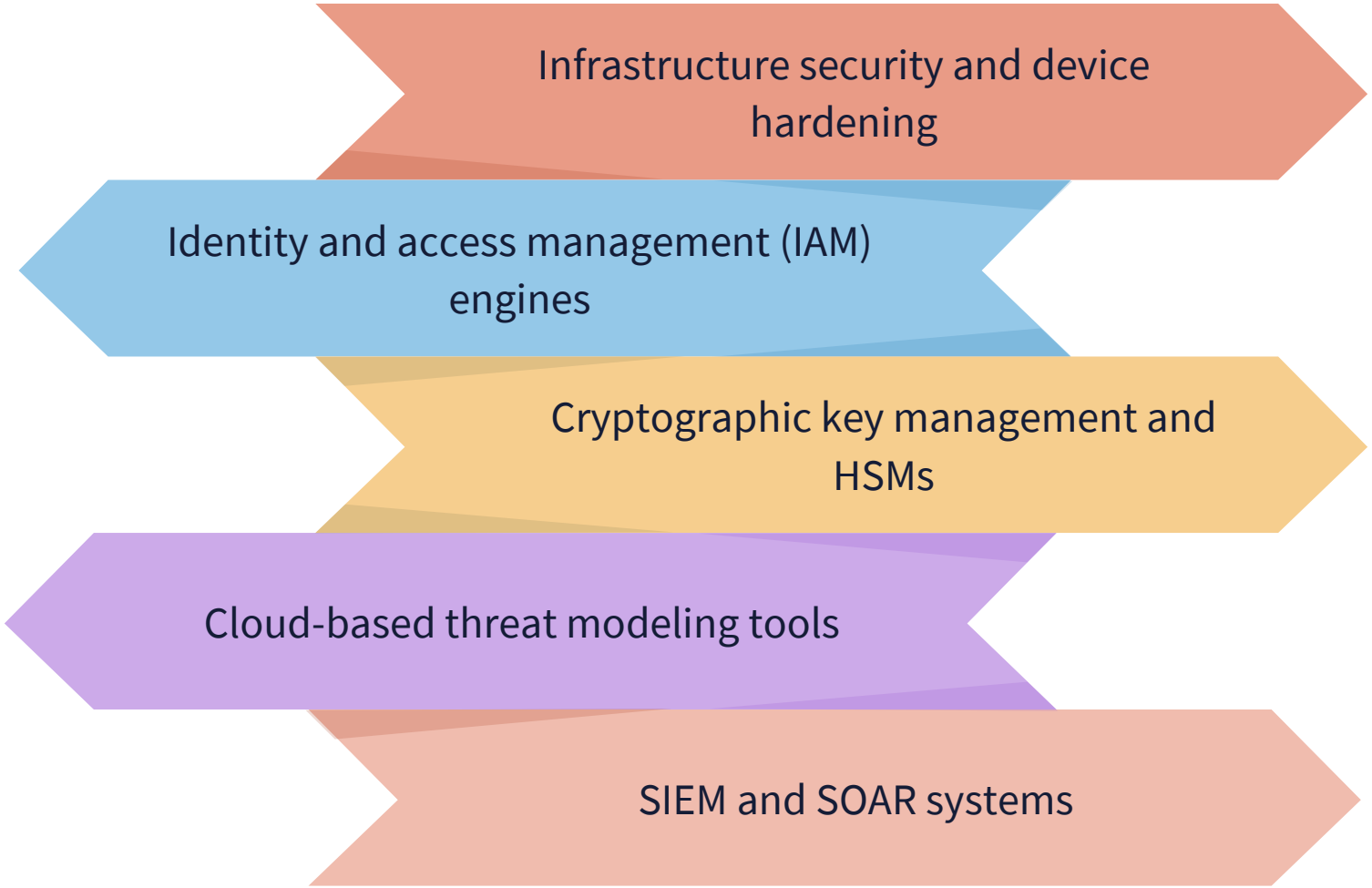
Physical

TECHNICAL CONTROLS

- Are security mechanisms that the specific systems run – either manually or, more often, automated and orchestrated
- Deliver confidentiality, integrity, authenticity, and availability protections
- Defend against unauthorized access or misuse
- Facilitate the detection of security violations and support security requirements for applications and data



COMMON TECHNICAL CONTROLS

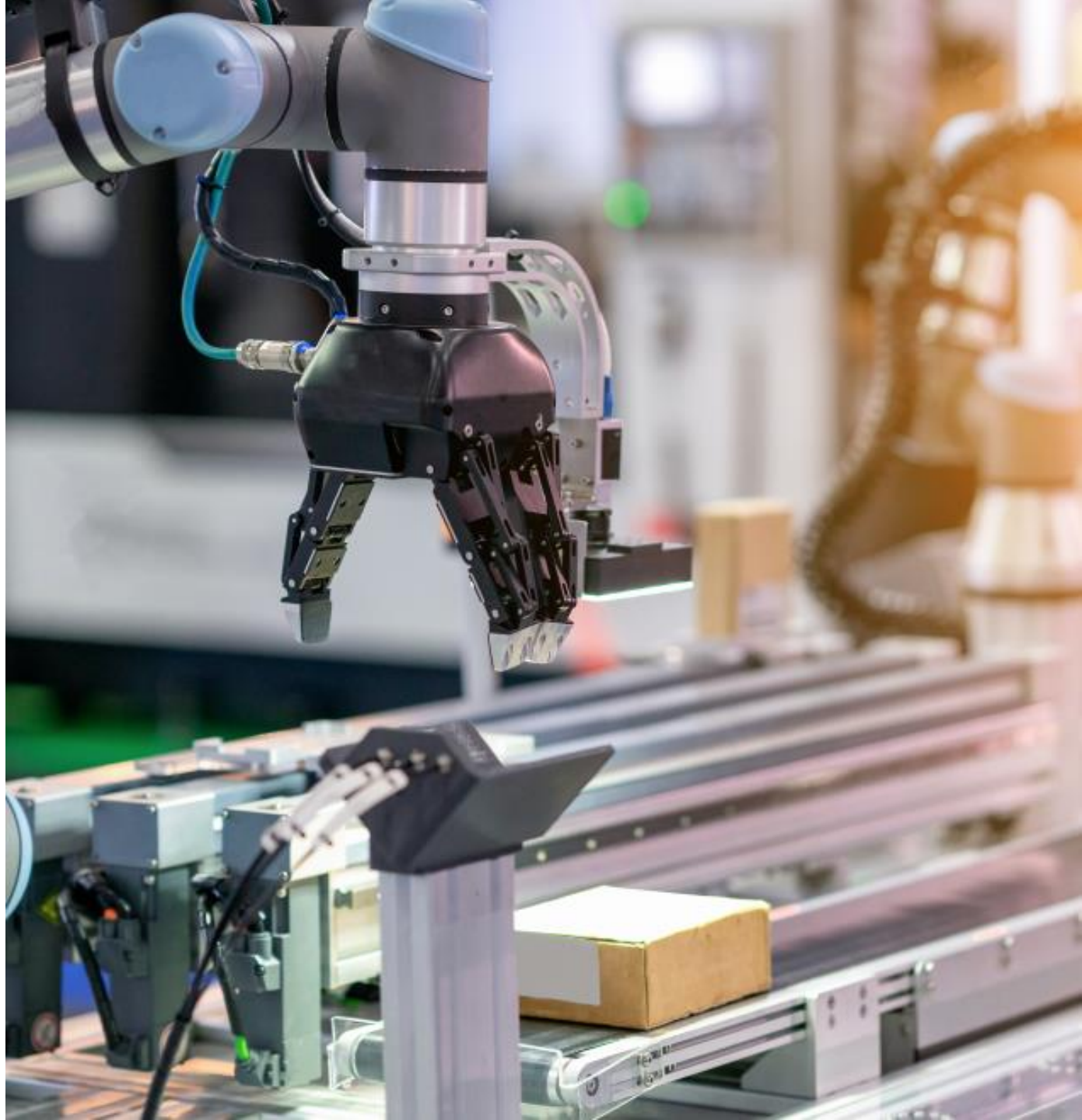


MANAGERIAL CONTROLS

- Managerial (also administrative) controls define policies, procedures, best practices, and guidelines
- They are usually more logical in nature
- Should be a published or printed definition of policies:
  - No piggybacking (tailgating)
  - Acceptable use policies
  - Best practices and guidelines
  - Password policies
  - Screening, hiring, and termination procedures
  - Mandatory vacations
  - Training and awareness

OPERATIONAL CONTROLS

- Operational controls support ongoing maintenance, due care, and continual improvement:
  - Optimizing the change and configuration management database
  - Performing tested patch management
  - Conducting awareness and training
  - Monitoring physical and environmental controls
  - Conducting incident response and disaster planning testing and drills
  - Performing software assurance initiatives
  - Managing mobile devices and mobile applications on an ongoing basis



PHYSICAL CONTROLS

- Physical controls are introduced to protect the campus, facility, environment, and people:
  - Various physical barriers
  - Guards and security teams
  - Cameras and surveillance equipment
  - Different types of sensors and alarms
  - Locking mechanisms
  - Secure safes, cabinets, cages, and areas
  - Mantraps and Faraday cages
  - Fire detection and suppression systems
  - Environmental controls

SECURITY CONTROL TYPES

SECURITY CONTROL TYPES

Preventative

Stops an attacker from successfully conducting an exploit or advanced persistent threat

Deterrent

Discourages an attacker from initiating or continuing an attack

Detective

Identifies an attack that is occurring as well as the steps of the kill chain

SECURITY CONTROL TYPES

Corrective

Restores a system to state before the negative event occurred; can simply rectify or correct an identified problem

Compensating

Aids controls that are already in place or provides a temporary stopgap solution

Directive

Consists of mandatory policies and regulations that are in place to maintain consistency and compliance

FUNDAMENTAL SECURITY CONCEPTS

Objectives

- Learn about gap analysis
- Define zero trust initiatives
- Explore deception technologies
- Examine preventative and detective physical controls
- Look at change management business and technical processes
- Describe documentation and version control

GAP ANALYSIS

- To know where you are and where you need to go as a secure organization, you must conduct gap analysis
- This technique will be applied to several security projects, plans, and initiatives throughout an entire career
- Information security gap analysis is a comprehensive appraisal that helps organizations determine the difference between the current state of their information security to specific industry requirements guidance and best practices

GAP ANALYSIS

- When performing a security gap analysis, one will better understand the status of the cybersecurity risks and vulnerabilities in the organization
- This type of risk assessment indicates where the technical, physical, managerial, and continuing operation controls need to be deployed
- It involves knowing what the residual risks are and what further physical and logical safeguards (if any) need to be acquired and implemented

COMMON SECURITY GAPS

- Weak and/or shared credentials
- Lack of tested patch management
- Violation of the least privilege principle
- Having no/unenforced acceptable use policies
- Poor physical security
- Configuration and deployment errors due to lack of change and configuration management
- Poor visibility and lack of proper auditing

ZERO TRUST

- Zero trust (ZT) is the term for an evolving set of cybersecurity initiatives that move defenses from static, network-based perimeters to focus on users, assets, and resources
- ZT assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership

ZERO TRUST

- Authentication and authorization (both subject and object) are discrete functions performed before a session to an enterprise resource is established (TCP/TLS)
- ZT embraces the principle of least privilege consistently across all resource classes and locations
- Segregation (separation) of duties and high visibility (SIEM/SOAR) are also emphasized

ZERO TRUST ADAPTIVE IDENTITY

- Adaptive identity is another key ZT component
  - It is also called adaptive authentication or risk-based authentication
- It is a method of access to data that matches user credentials with the risk of the requested authorization
- It delivers support for multiple classes of consumers and participants, whose roles and identity may evolve to meet rapidly evolving ecosystems and environments
- Offers ease of maintenance and operation while being agile and easy to modify

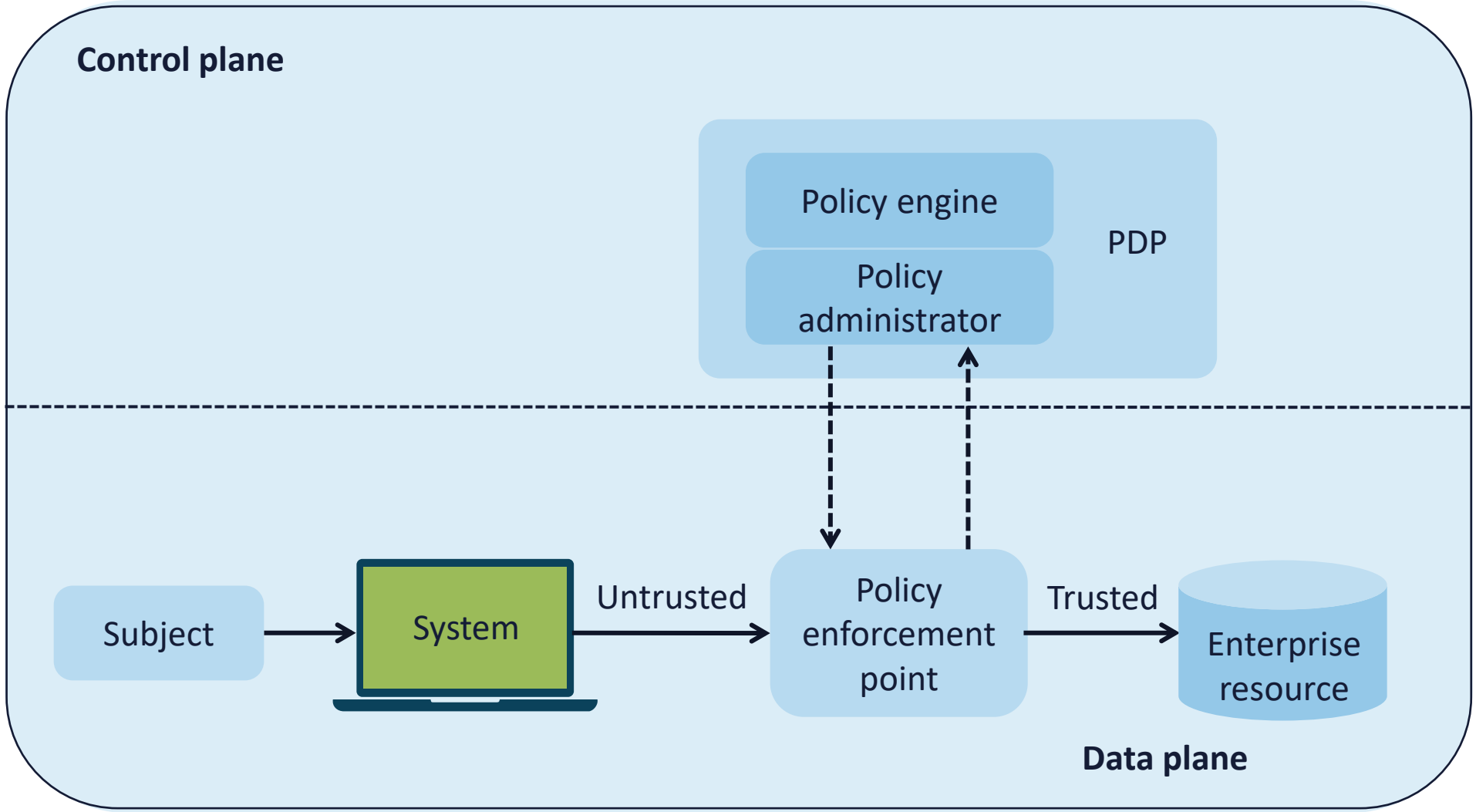
ZERO TRUST THREAT SCOPE REDUCTION

- Another main goal of ZT is threat scope reduction and risk avoidance
  - Reduced scope of threats to support agility and support complexity
  - Increased complexity and number of communication patterns, increasing difficulty of addressing through a data and asset-centric approach

ZERO TRUST CONTROL PLANE

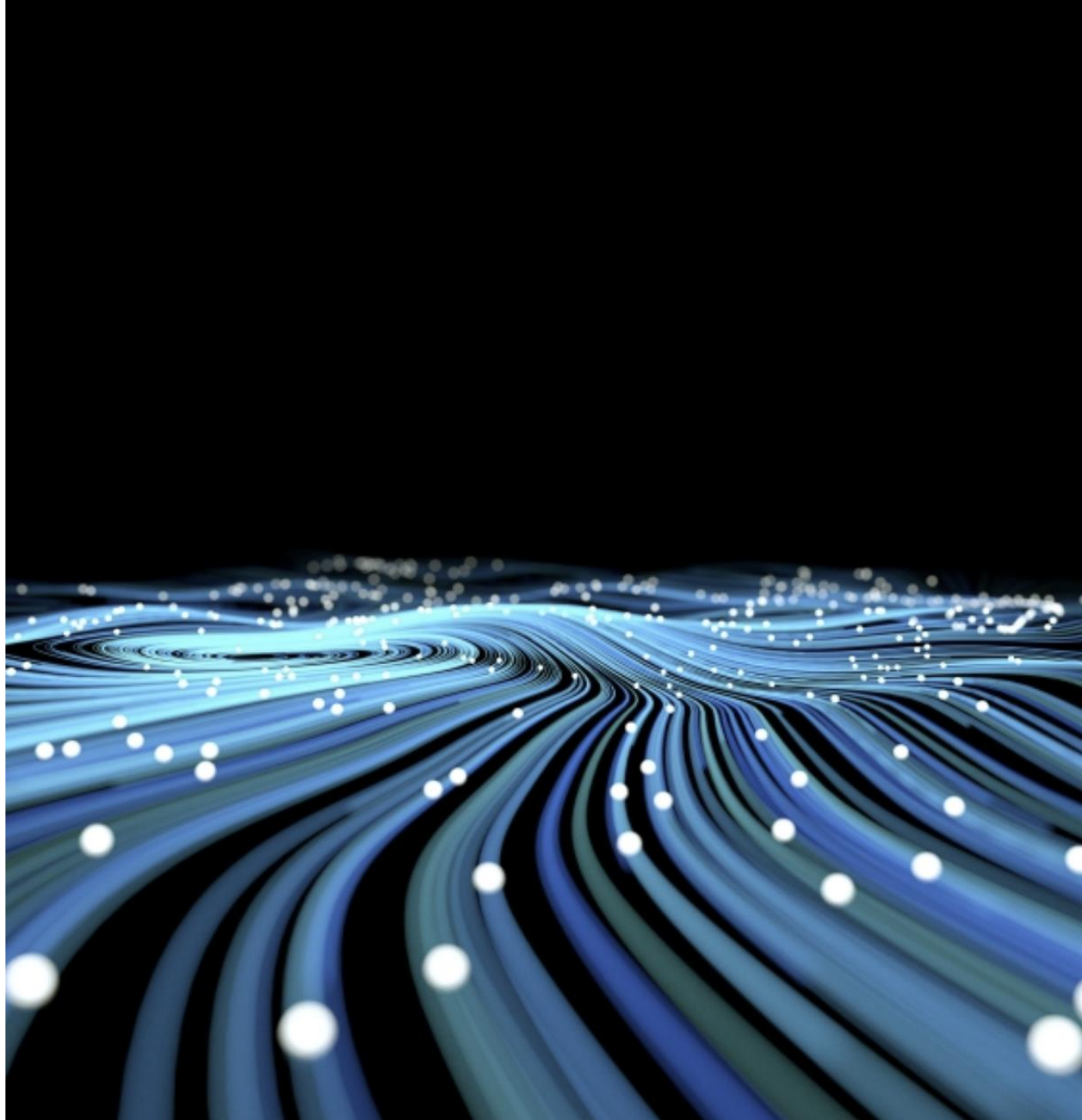
- The ZT control plane is separate from the data plane and contains the **policy decision point (PDP)**, which includes:
  - The **policy engine (PE)**, which uses the enterprise policy-driven access control (as well as input from external sources) to grant, deny, or revoke access to resources
  - The **policy administrator (PA)**, which enables and/or shuts down the communication path between a subject and a resource via commands to associated **policy enforcement points (PEPs)**
  - The PA communicates with the PEP when creating the communication path via the control plane

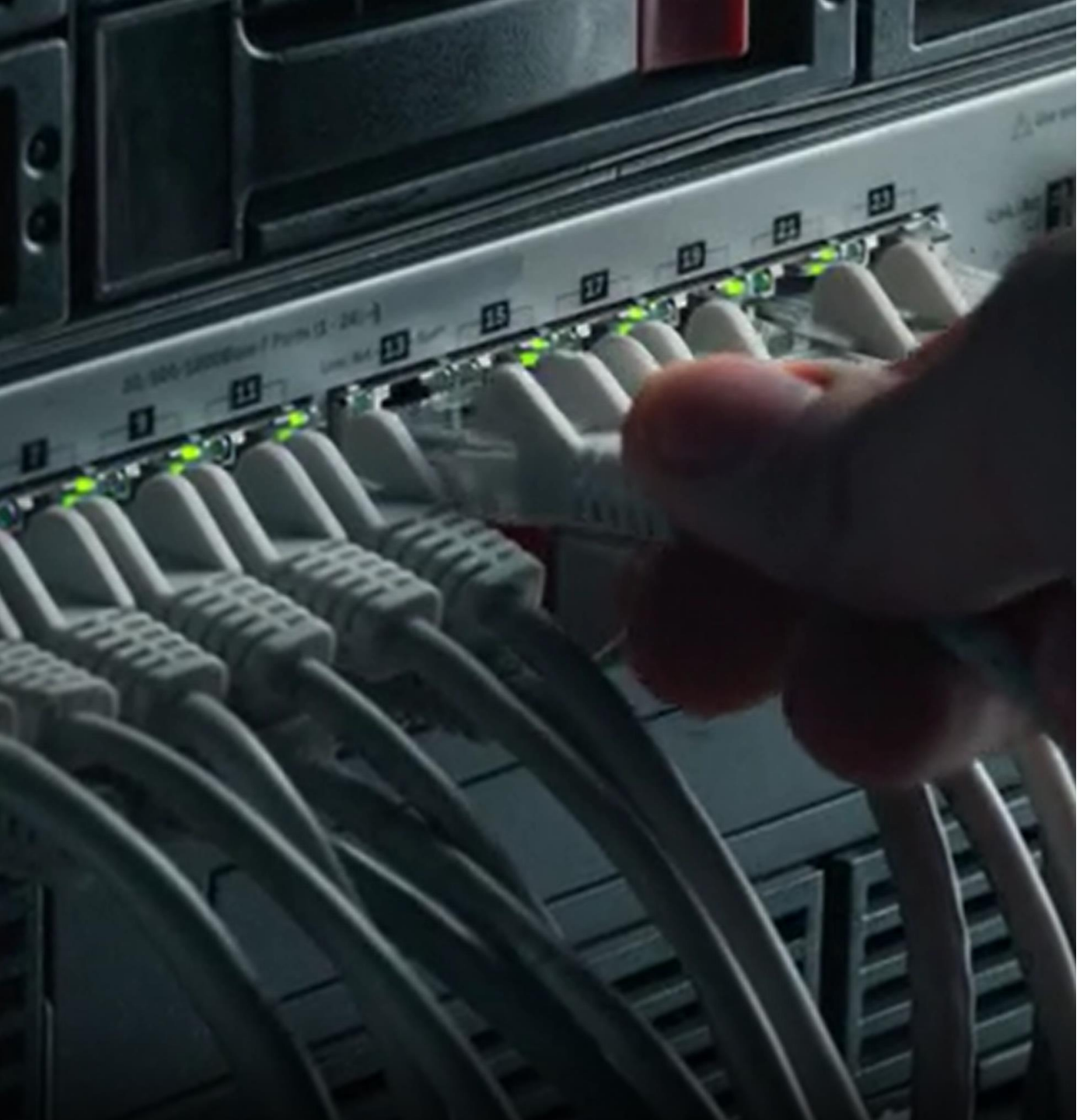
ZT ARCHITECTURE



ZERO TRUST DATA PLANE

- The zero trust data plane is defined by explicit trust zones, which could include
  - Data centers
  - DMZs (public access zones)
  - The public Internet
  - Cloud computing subnets such as private or VPN-only
  - Honeynets

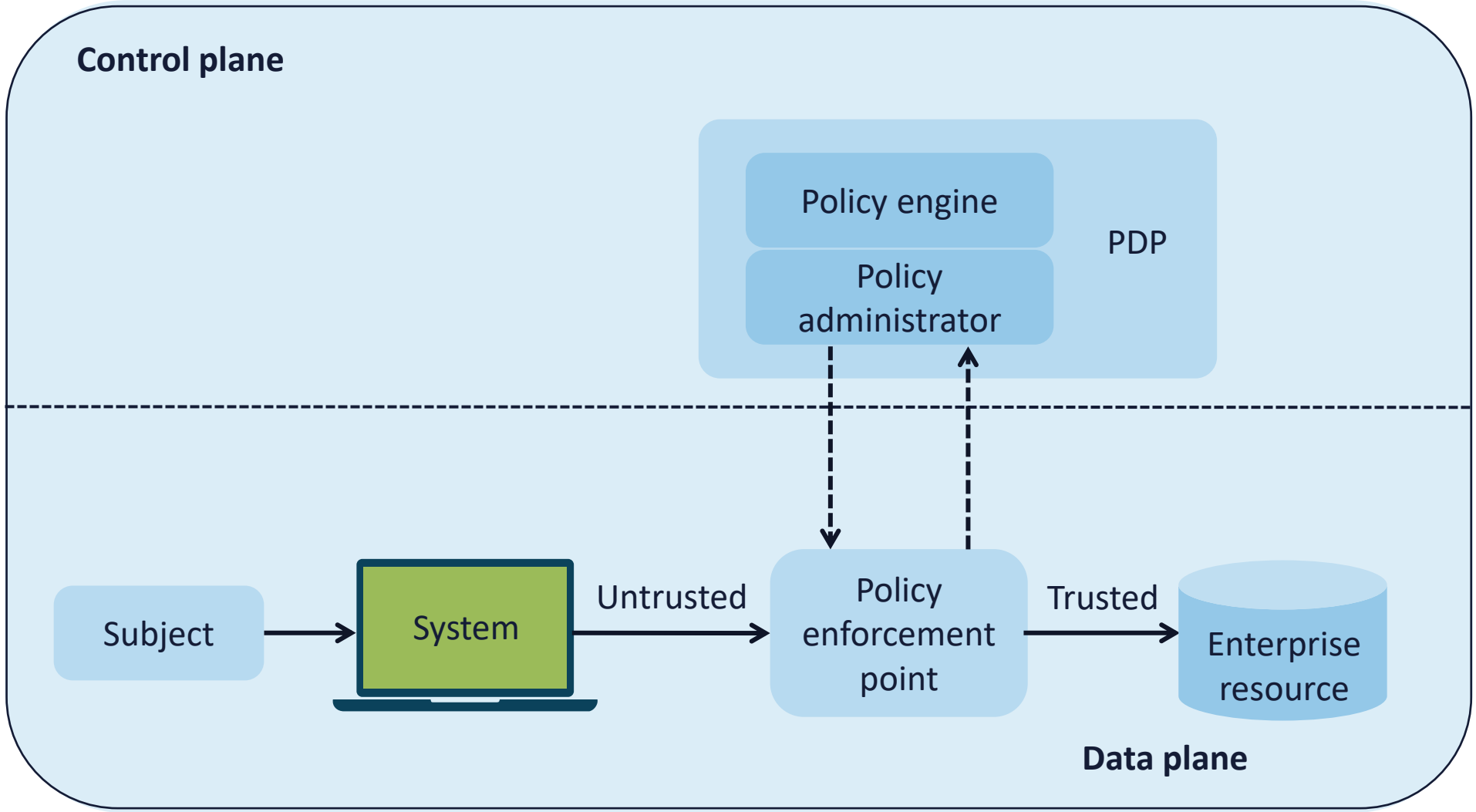




POLICY ENFORCEMENT POINTS (PEP)

- Network PEPs:
  - Edge routers
  - Edge firewall appliances
  - SDP access gateways
  - Network L2/ML switches
  - Authentication proxy servers
- Application PEPs:
  - API gateways
  - Resource groups
  - Network VLANs
  - Code repositories
  - Cloud services

ZT ARCHITECTURE



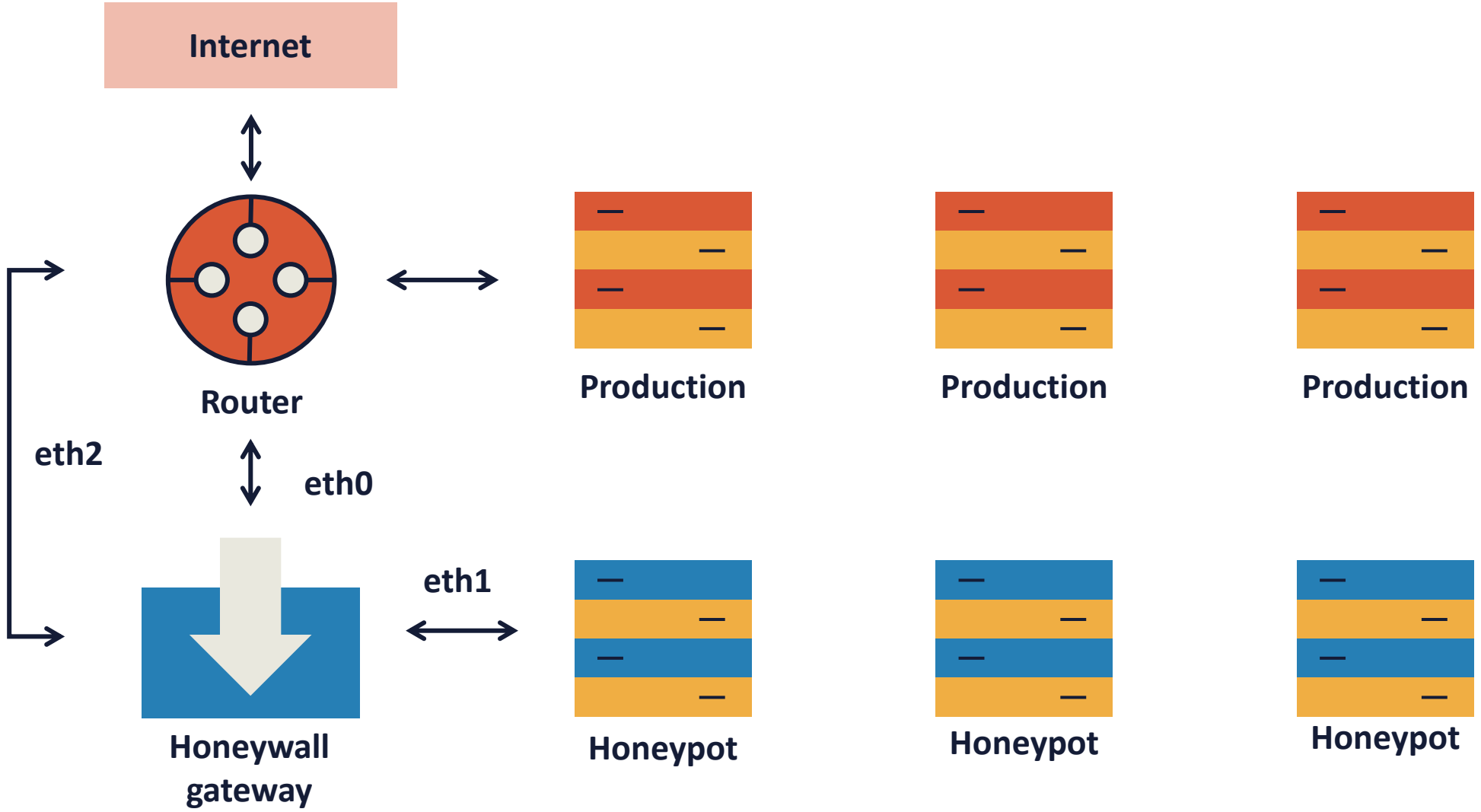
DECEPTION TECHNOLOGIES: HONEYPOT

- A honeypot is a system (e.g., a web server) or resource (e.g., a file on a server) that is designed to be attractive to potential attackers and intruders, like honey is eye-catching to bears
- Modern systems are often running as a virtual machine in a type 1 hypervisor such as a VMware solution
- They are strategically placed in parallel to public access or demilitarized zones where public-facing servers are typically placed

HONEYNETS

- A honeynet can simply be considered a "network of honeypots"
- It is also set up with intentional vulnerabilities hosted on decoy servers and services to attract or redirect attackers
- The primary purpose is to test network security by inviting attack patterns and "kill chains"
  - This helps security teams analyze an actual attacker's activities and methods to improve network security

HONEYNETS


Internet
Router
eth2
eth0
eth1
Honeywall gateway
Production
Production
Production
Honeypot
Honeypot
Honeypot

HONEY FILES AND HONEY TOKENS

- The compromised privileged insider is the number one internal structured threat for most organizations
- Honey files and tokens are strategically placed artifacts and files meant to allure the suspect into exposing themselves as part of an internal investigation
- They are also valuable in the discovery of attackers who are deep into the kill chain phases
- Common examples are access keys and credentials to valuable cloud-based assets and database entry points

PREVENTATIVE PHYSICAL SECURITY CONTROLS

- Before security professionals can focus on technical and operational countermeasures, they must be certain that these are deployed in a physically secured property, facility, and environment
- Although detective and deterrent controls are important, prevention is critical for protecting all types of assets

FENCE BARRIERS

- Most organizations will have protective fence barriers around the perimeter to deter or prevent individuals from unauthorized entry and exit
- Fences may only be used in certain zones or areas to protect junction boxes, generators, dumpsters, and shredding service pickup points
- Fences can be of varying heights and barbed depending on the locale
- Electrified fences and signage are also common for high security properties and facilities (e.g., airports, prisons, military installations)

GATES

- Fences are often combined with entry/exit gates of varying strength and guarding
- Barricade gates and tire shredders are common
- Types of gates in the U.S. include
  - Class I: Residential gate operation
  - Class II: Commercial, such as a parking lot or garage
  - Class III: Industrial/limited access (e.g., warehouses, factories, docks)
  - Class IV: Restricted access operation requiring supervisory control

BOLLARDS

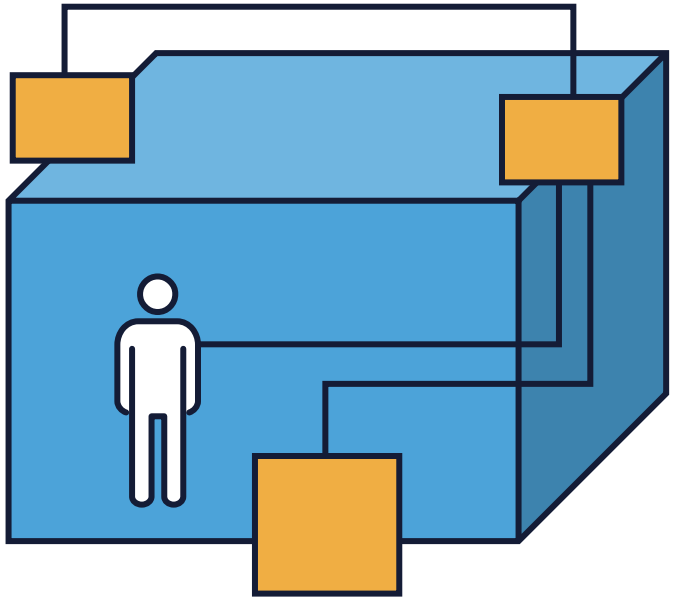
- Bollards are strategically placed pylons meant to redirect pedestrian traffic or prohibit vehicles from entering certain areas, such as the foyer of an office building
- They can be permanent or temporary pillars
- They are typically made of concrete or strong metal
- High-tech bollards can be mechanical and include cameras and sensors

ACCESS CONTROL VESTIBULES

- Access control vestibules are typically areas that are fortified with forced entry-resistant and bullet-resistant security glazing
- These fortified entryways serve as formidable barriers to unauthorized access that go beyond traditional security measures
- Access control vestibules are also known as security or mantrap vestibules and are a highly effective means of hardening commercial security, typically through a series of interlocking doors

MANTRAPS

- There is an entry and exit door but only one door can be open at a time
- One person at a time – no piggybacking (tailgating):
  - Person can be identified and authenticated
  - Provide credentials and license or passport
  - Can include biometric readers
  - CCTV and intercom systems are often used
  - Security guard behind bullet-proof glass
  - Person is eventually allowed in through a strong door with electronic locks

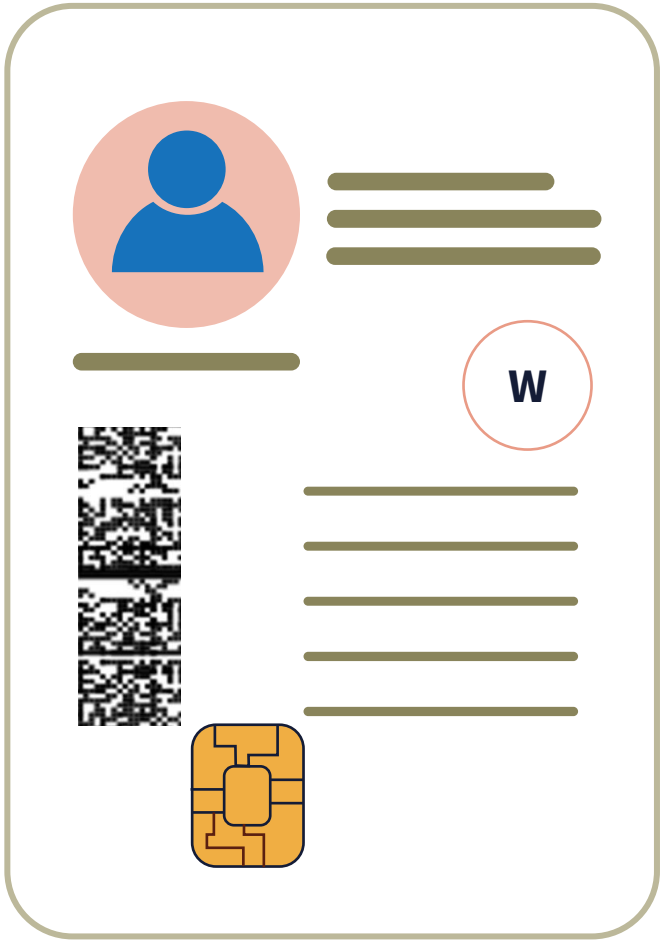


ACCESS BADGES AND CARDS

- Access badges and cards represent another "something you have" authentication factor
- Many organizations will have all guests register at a reception area security desk:
  - Collect and input identification information in a visitor log
  - Distribute temporary access cards or badges
  - Have a camera station for pictures for a temporary badge
- There should be a "no tailgating (piggybacking)" policy at all access points

COMMON ACCESS CARD (CAC)

- Expiration date
- Federal identifier
- Affiliation
- Service/agency
- Color indicator
- Pay grade
- Rank
- Integrated circuit chip



SECURITY GUARDS

- Security guards are typically 24x7, but could just be present during business or non-business hours
- They are a security control of multiple types:
  - Detective
  - Deterrent
  - Preventative
- They can provide rapid security response if an intrusion or incident occurs
- Robot sentries are rapidly replacing humans in certain scenarios

SECURITY GUARD CONSIDERATIONS

- Are they hired, contracted, or freelance?
- Do they need to be certified/licensed?
- Will they be armed or unarmed?
- What is the impact on insurance policies?
- Is the organization directly involved with screening and background checks?
- Where are they stationed on the campus?
- Who provides the ongoing training?

VIDEO SURVEILLANCE

- Cameras and video surveillance provide a way to monitor and record the property perimeter for intruders and potential attackers
- They are considered detective physical controls, but the mere presence may also be a deterrent
- Video surveillance offers a way to record intruders in action with recordings
- Alerts should be triggered when a camera is disabled

VIDEO SURVEILLANCE CONSIDERATIONS

- The systems will be indoor and outdoor webcams or CCTV systems
- May be closed-circuit to a security operations center (SOC)/linked to a third-party vendor
- It is imperative to transfer media to a safe and secure location
- Industrial camouflage involves cameras and surveillance devices hidden in landscaping elements, statues, and tall trees
- It should be combined with various lighting solutions, both of which can have "dead spots"

LIGHTING

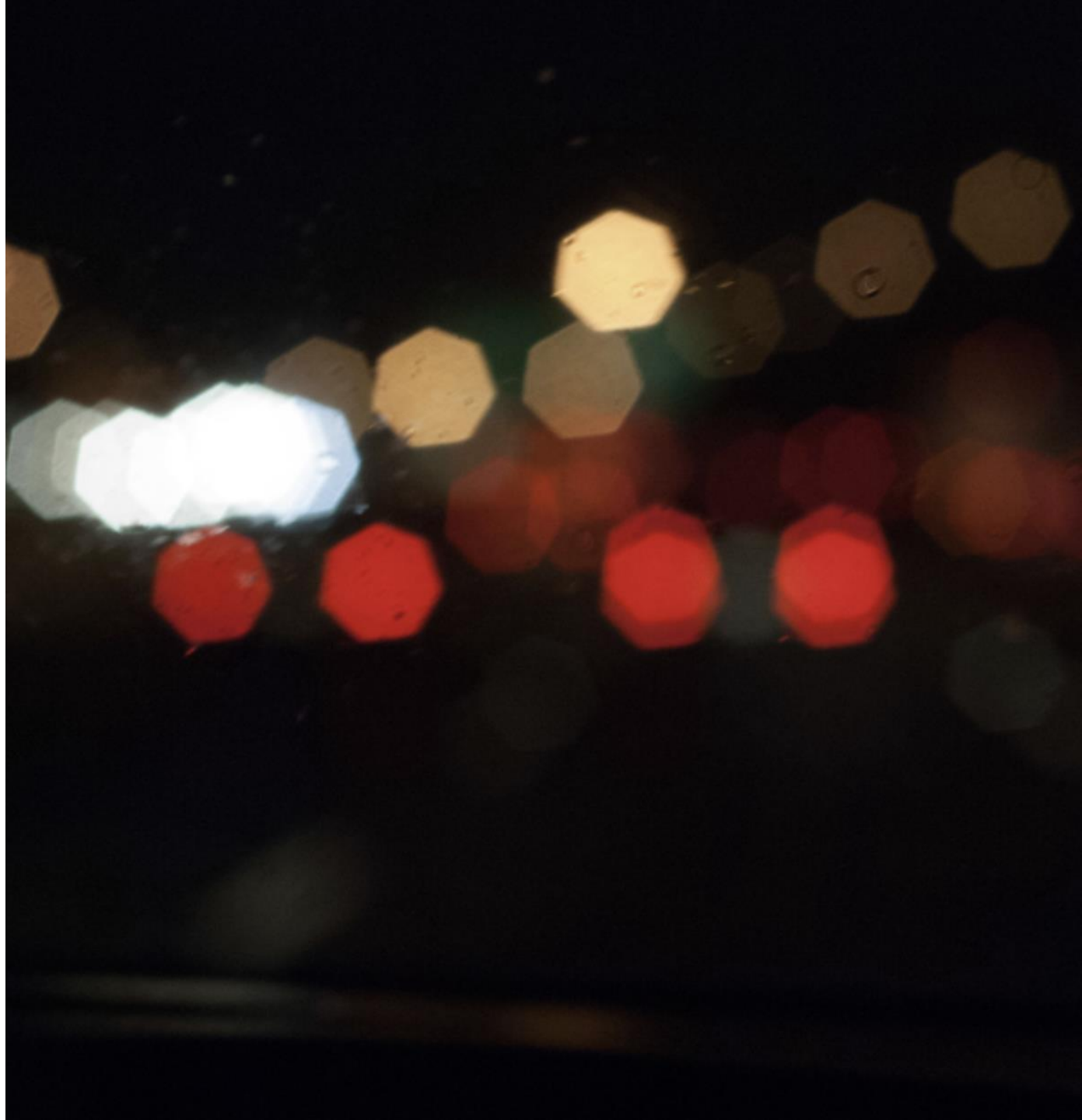
- Lighting can enhance other security controls such as cameras, security guards, and sensors
  - They should start at the perimeter and be used in every defense-in-depth mechanism
- Some modes of lighting can be mercury vapor, sodium vapor, quartz, and LEDs

SECURITY LIGHTING

- **Continuous lighting** is the most familiar form of outdoor security lighting and can provide greater projection and control
  - The glare of continuous (barrier) lighting originated in prisons and correctional institutes and is still in use today
- **Stand-by lighting** systems are designed for reserve or stand-by use or to supplement continuous systems
  - These systems are engaged either automatically or manually when the continuous system is inoperative or when there is a need for extra light

SECURITY LIGHTING

- **Moveable lighting hardware** is manually operated and typically is made up of moveable search or flood lights located in chosen places, which require temporary lighting
  - The moveable system is also used to supplement continuous or stand-by lighting and is often used at construction sites
- **Emergency lights** are used in times of power failure or other emergencies when other systems are inoperative – often gas-powered generators or batteries



TYPES OF SENSORS

- Photoelectric – a break in a light beam
- Passive infrared – detecting infrared light
- Vibration – a change in the level of vibration
- Acoustical – noise detection of a change in sound waves
- Microwave – a change in high-frequency radio waves
- Electro-mechanical – a break in electrical circuit
- Electrostatic – a change in an electrostatic field
- Moisture and temperature detection – for server rooms and data center environmental control

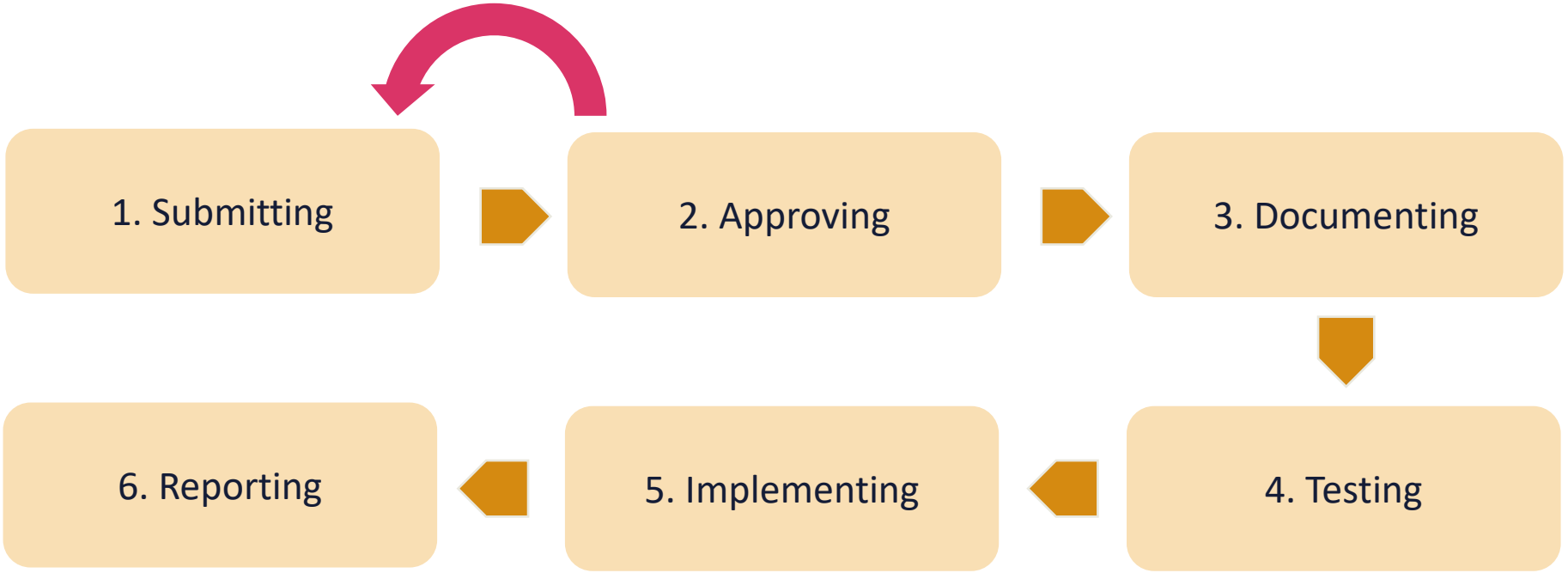
SENSORS TRIGGER ALARMS

- A static or flashing light on the display panel in the security room or operations center
- Bells ringing or horns blaring
- Sending a text notification to an interested party
- Sending an email message
- A silent alarm to a security firm or local law enforcement
- A telephone or cellular call to a software program or live attendant

CHANGE MANAGEMENT

- Change management is the methodical approach to handling the transition or modification of an organization's goals, processes, or technologies
- The purpose is to implement strategies for carrying out change, controlling transformations, and assisting individuals in adapting to change
- Change management is also referred to as the change control practice
- Typically, configuration management occurs first to establish a baseline before standard, normal, and emergency changes occur

CHANGE MANAGEMENT LIFECYCLE



CHANGE CONTROL BUSINESS PROCESSES

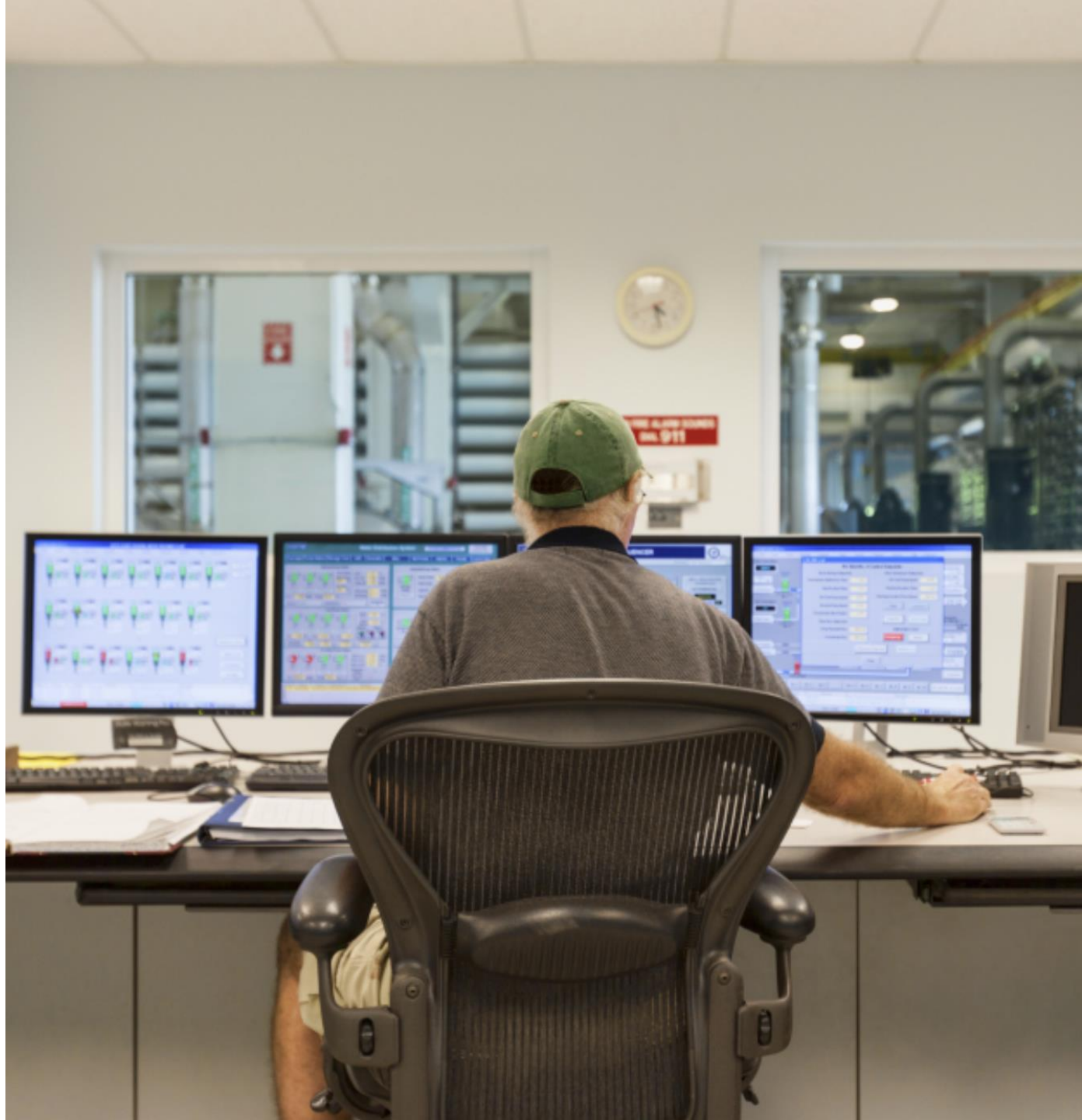
- The **approval** process should be a flexible and highly iterative phase of the lifecycle
- **Ownership** of the physical or logical asset must be considered and is driven by the access control model
- All **stakeholders** should be either involved based on the RACI model
  - Responsible, accountable, consulted, informed

CHANGE CONTROL BUSINESS PROCESSES

- A **change impact analysis** compares two states (the current and future state) of a change to identify what is changing, who is impacted by the change, and what needs to be communicated to the impacted
- The process involves identifying and categorizing who and what will be affected, assessing the degree of change occurring within these areas, and describing the change
  - This last activity folds into stakeholder analysis, communication analysis, and strategies

CHANGE CONTROL BUSINESS PROCESSES

- A change **backout or fallback plan** is a recovery point, and it must be in place during both the testing plan and implementation phase
  - Make small individual changes instead of several impactful changes
- **Maintenance windows** are typically used to show times during which changes should be scheduled
- A **standard operating procedure (SOP)** offers precise directions and detailed instructions needed to perform a specific task or operation consistently and proficiently



CHANGE MANAGEMENT TECHNICAL IMPLICATIONS

- **Allow/deny lists** are used with change control in line with the access control model to dictate which subjects are allowed to make changes or not
  - An allow list is a permissive control
  - A deny list is a restrictive control
- By implementing least privilege and separation of duties, certain activities and areas will be restricted

CHANGE MANAGEMENT TECHNICAL IMPLICATIONS

- **Downtime** relates to high availability, which is an aspect of resiliency
- **Availability** consists of planned and unplanned downtime (e.g., an outage) and must be considered with technical change management when making modifications or performing migrations
- Other considerations are a service restart, application restart, legacy applications, and all dependencies

DOCUMENTATION AND VERSION CONTROL

- Organizations must document using a well-established tagging and labeling schema that maps to a configuration management database (CMDB), such as ServiceNow
- A configuration management system (CMS) is a set of data, tools, utilities, and processes used to support configuration management
  - Relational databases have been used historically
  - NoSQL/document databases are emerging as a common solution
  - You could leverage a CSP service, such as Amazon Redshift data warehousing or DynamoDB

DOCUMENTING WITH A CMDB

- A configuration management database is not a typical data warehouse
- It plays a critical role in several IT management initiatives, like IT service management (ITSM) and IT asset management (ITAM)
- It helps various IT services to better align with business needs by providing current and accurate data for
  - Change and patch management
  - Incident and problem management
  - Availability management
  - Release and deployment management

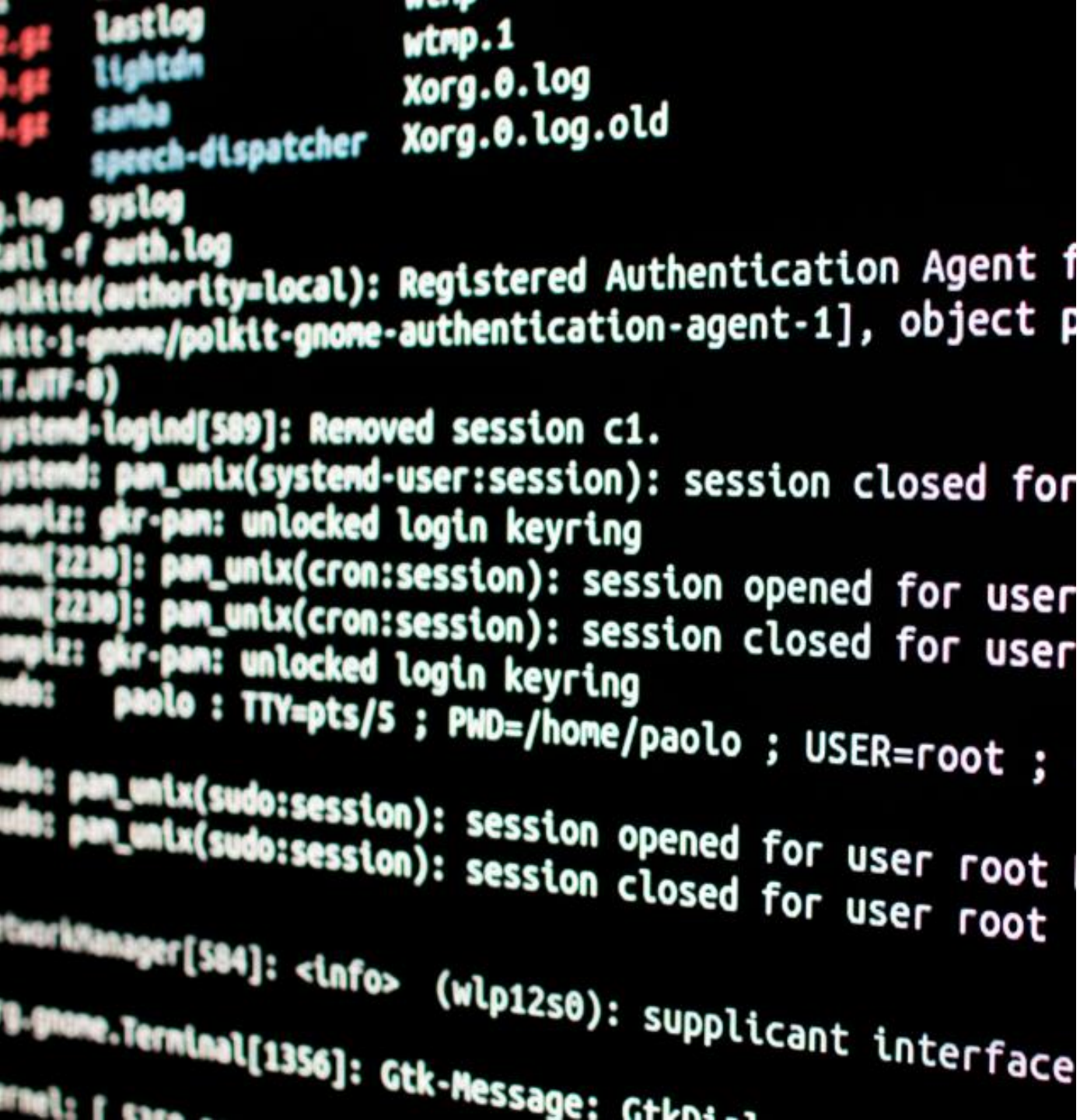
VERSION CONTROL

- Version control and change management procedures are important to both the operations team and the security team
- Version control applies to
  - Operating system builds
  - Application updates
  - Device drivers
  - Licensing updates
  - Various upgrades and patches
  - Container packages and microservices
  - Firmware updates
  - Trusted platform modules
  - Component updates

PRACTICAL CRYPTOGRAPHY

Objectives

- Compare symmetric and asymmetric cryptography
- Learn about encryption levels as in full disk, partition, file, volume, database, and record
- Examine hashing, salting, HMACs, and key exchange
- Explore digital signatures, certificates, and PKI
- Observe various cryptographic tools
- Understand blockchain technology



CRYPTOGRAPHIC SERVICES

- **Confidentiality**
  - Hiding the data at rest, in transit, and/or in use from unauthorized principals
  - It typically involves a system or algorithm that converts plaintext data into ciphertext
- **Integrity**
  - Ensures the data has not been altered while at rest or in transit
- **Non-repudiation**
  - Ensures the original sender cannot deny sending data or engaging in a digital transaction

SYMMETRIC KEY CRYPTOSYSTEMS

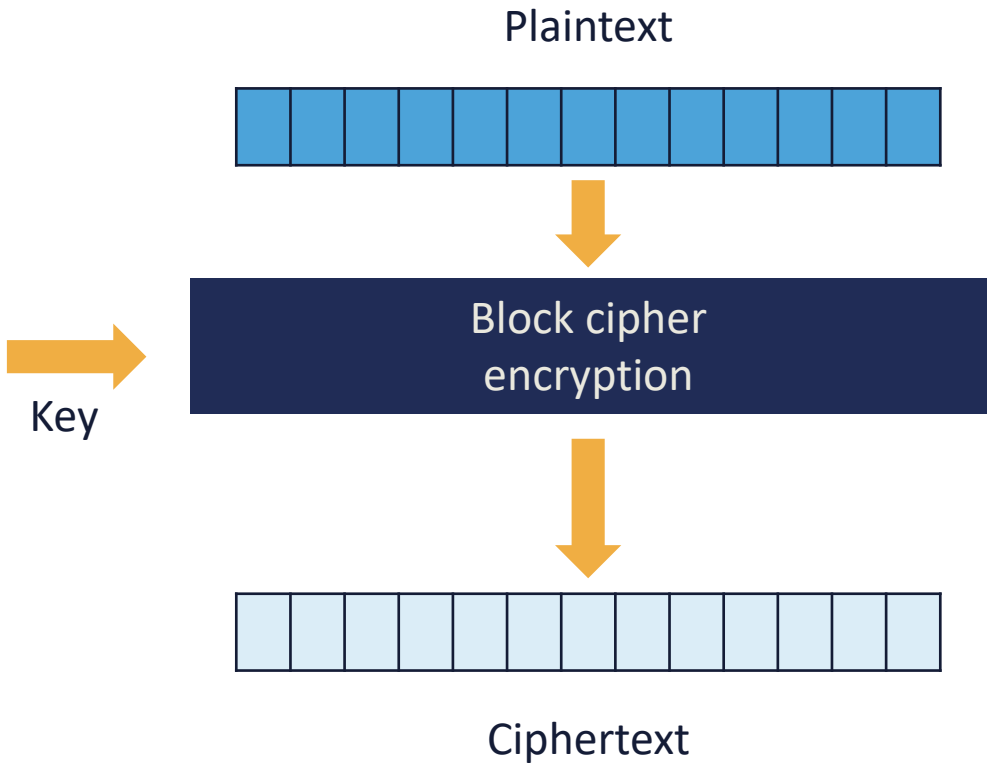
- This historic form uses the same key to encrypt and decrypt
- Efficient, fast, and handles high data rates of throughput
- Computationally inexpensive
- Deploys shorter key lengths (40 to 512 bits)
- Primarily used to protect data at rest

SYMMETRIC KEY CRYPTOSYSTEMS

- Key management is more complex unless using hardware security modules (HSMs) or cloud key management services
- There is no built-in origin authentication
- Symmetric systems do not scale well unless a cloud key management service is used
- Most popular algorithms are AES-CBC-128/256 and AES-GCM-128/256

BLOCK CIPHERS

- Operates on fixed blocks of data (bits) based on key size
- 64, 128, and 256-bit keyspaces are common
- Messages bigger than the key size are broken into blocks the size of the key and must include padding
- Common block ciphers:
  - DES
  - 3DES-EDE
  - AES-CBC
  - AES-GCM
  - Blowfish



STREAM CIPHERS

- Operate on a continuous stream of plaintext data by encrypting one bit or byte at a time
- Plaintext bits are typically XORed with keystream bits
- Keystream = random bits, bytes, numbers, characters
- Faster and less complex than block ciphers
- Modern ciphers can work in a block or stream mode or both:
  - FISH
  - CryptMT
  - Scream
  - Cryptographic hashing

STREAM CIPHER EXAMPLE

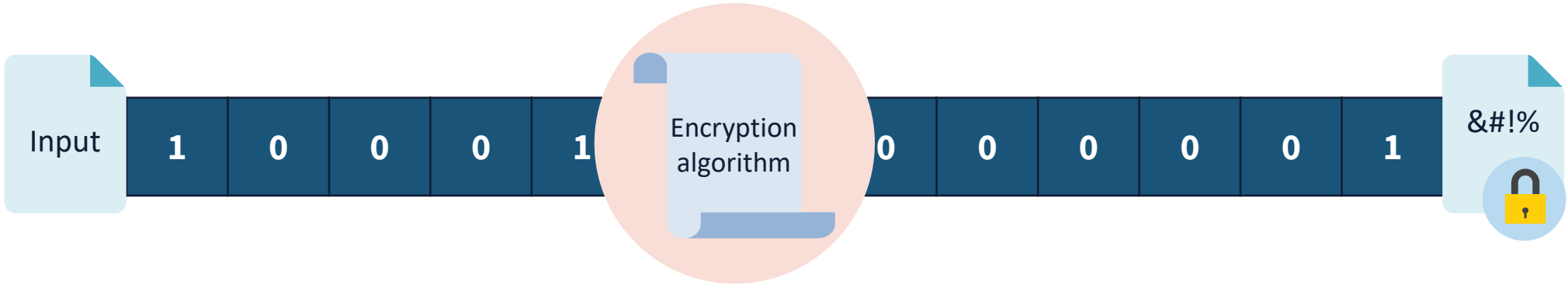
- Alice wants to use a stream cipher to encrypt the letter "A"
- In ASCII, the letter "A" has the value of 65 = 1000001
- The first cipher stream bits are 0101100
- We perform an XOR function (Modulo 2 addition)

  1000001 = A

  XOR

  0101100

  1101101 is the result
- The letter "A" becomes ciphertext "m" (ASCII value 109)

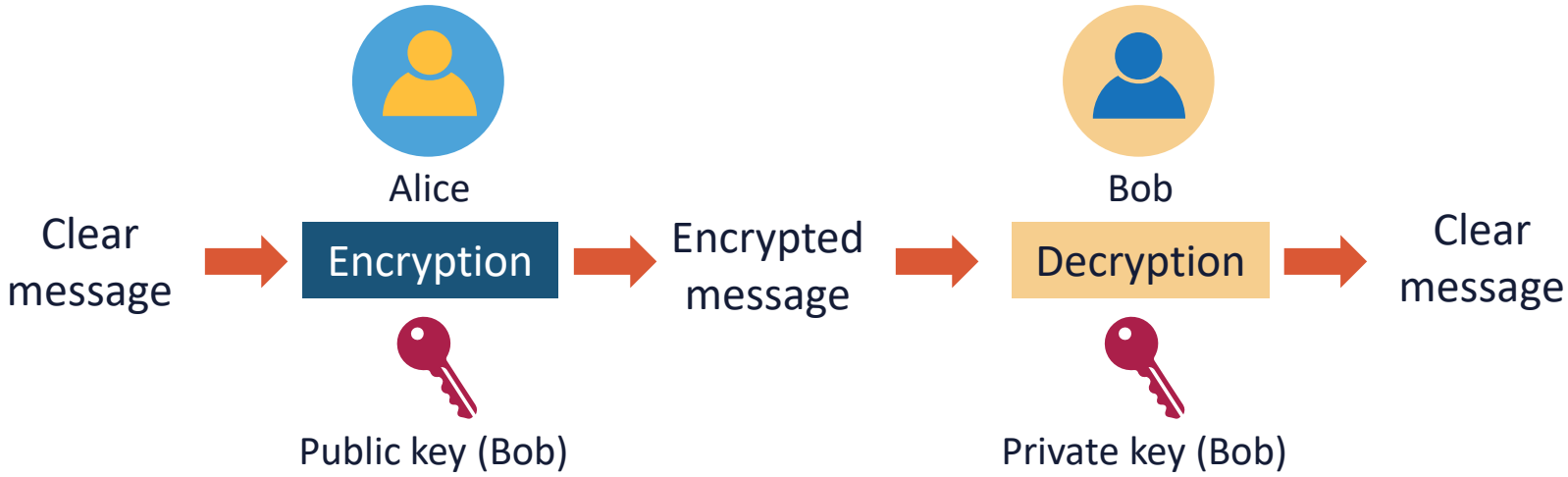


ASYMMETRIC KEY CRYPTOSYSTEMS

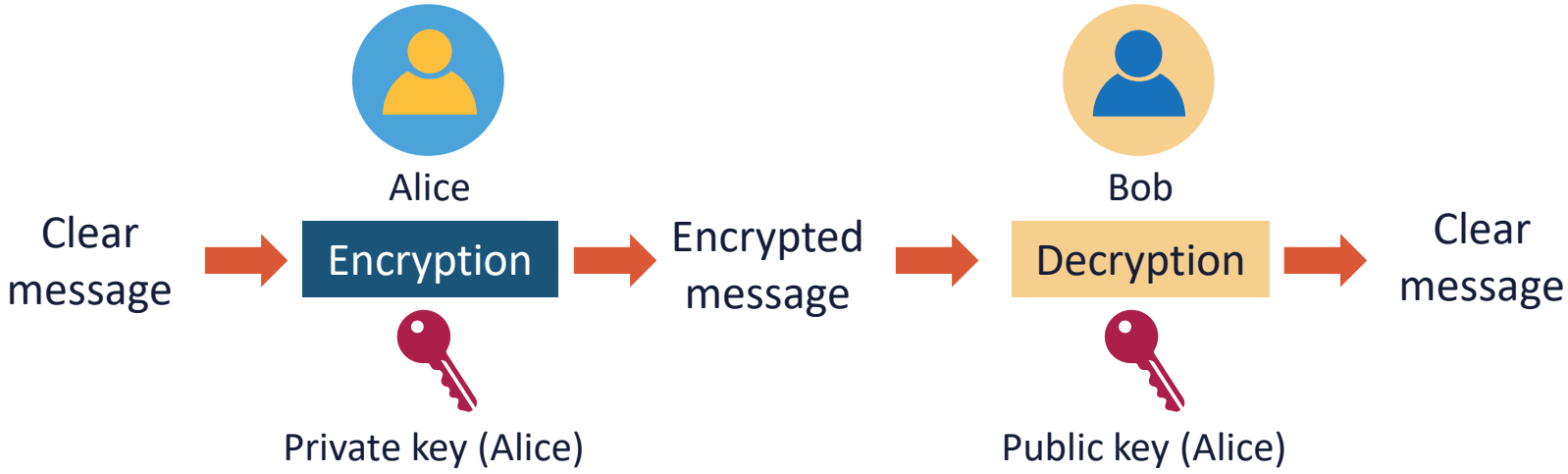
- Uses a mathematically related pair of a public and private key
  - If one is used to encrypt, the other is used to decrypt
- Public key infrastructure (PKI) enables efficient key management and scalability
- Often used for digital signatures and key exchange
- Employs longer key lengths than symmetric (up to 4096)
- Slower and more computationally expensive

ASYMMETRIC KEY CRYPTOSYSTEMS

- Confidentiality
  - Encrypt with public key
  - Decrypt with private key



- Origin authentication
  - Encrypt with private key
  - Decrypt with public key



POPULAR ASYMMETRic (PUBLIC KEY) ALGORITHMS

- RSA (Rivest–Shamir–Adleman) – the most widely used algorithm for securing communication and data encryption
- Diffie-Hellman key exchange – a protocol for securely exchanging cryptographic keys over an untrusted network
- Elliptic curve cryptography (ECC) – an algorithm based on the algebraic structure of elliptic curves over finite fields
- Digital signature algorithm (DSA) – a standard based on the mathematical concept of modular exponentiation and discrete logarithm problem

FULL DISK ENCRYPTION

- Full disk encryption (FDE) is the process of encoding all user data on a device using an encrypted key
- Also called whole disk encryption – the master boot record (MBR) (or comparable) that includes code that loads the operating system is not encrypted
- Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk

PARTITION ENCRYPTION

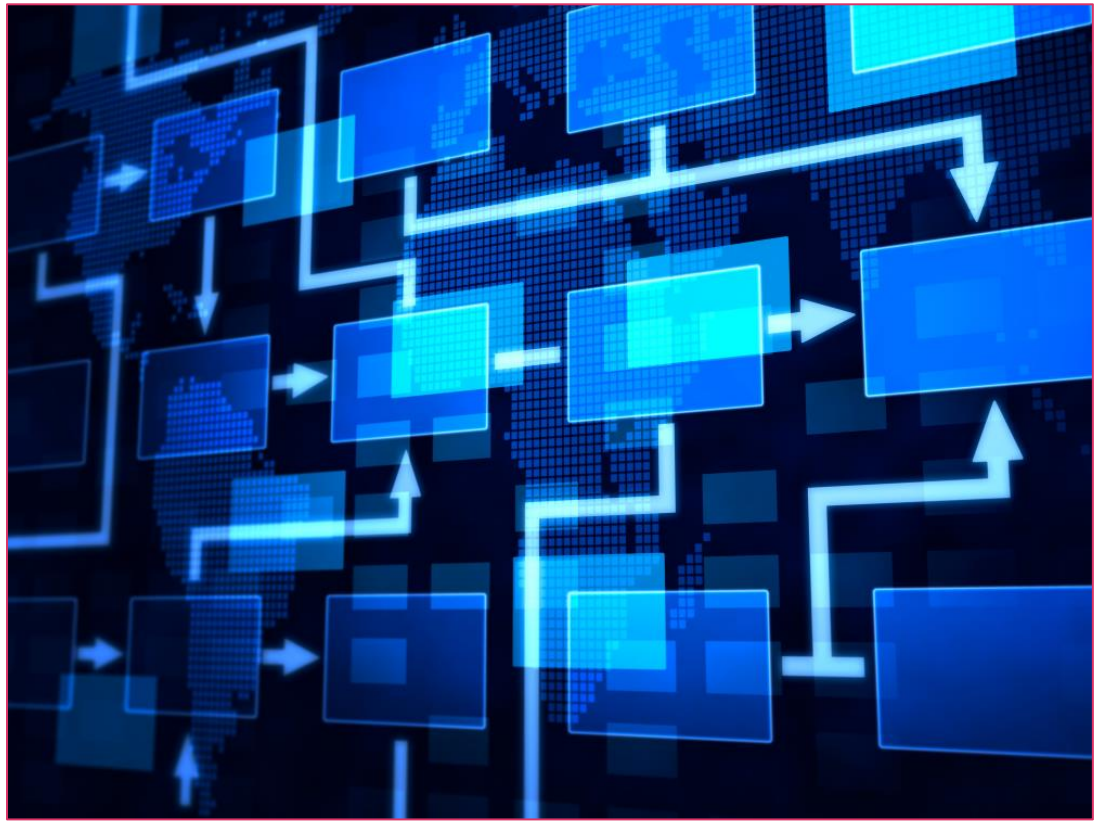
- Encrypted partitions are disk partitions that are protected with encryption keys to prevent unauthorized access to the data on the drive
- One advantage of encrypting only a partition instead of the whole drive is that you can encrypt/decrypt the partition while using the system for other tasks
- If one only encrypts a data partition, however, sensitive data can remain in temporary files or swap files in a non-encrypted partition

FILE ENCRYPTION

- File-level encryption enables the protection of individual files by encrypting them
- This technique is often utilized when there are specific files that need an extra degree of security or contain very sensitive information
- Encrypting individual files offers more control over access and assures that even if one file is cracked, the others will still be safe

VOLUME (BLOCK) ENCRYPTION

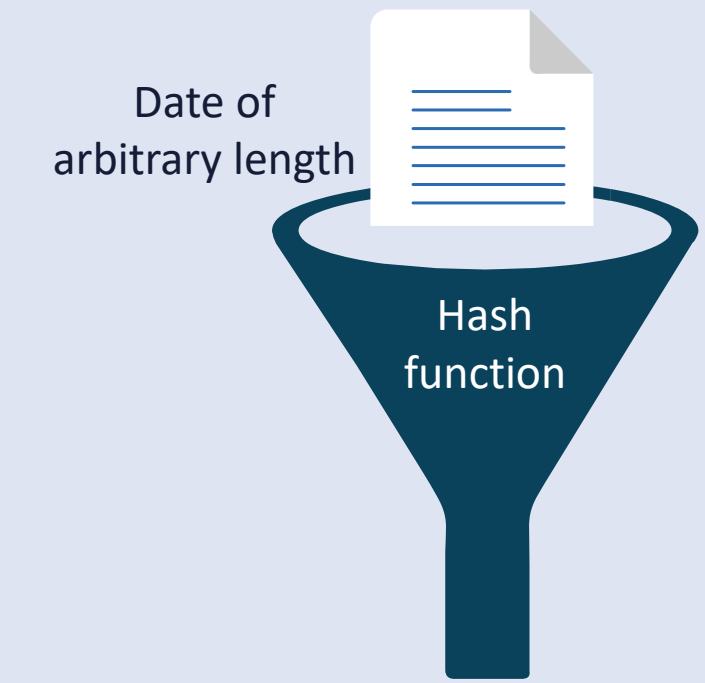
- Volume encryption targets a section of the physical drive, which is defined as a separate partition or "volume"
- It provides a choice to encrypt different volumes, whereas with disk encryption, you can only encrypt everything
  - Volume encryption can help save time and provide greater flexibility
- If a single volume occupies the entire hard drive, then volume encryption will function the same way as full disk encryption



DATABASE AND RECORD ENCRYPTION

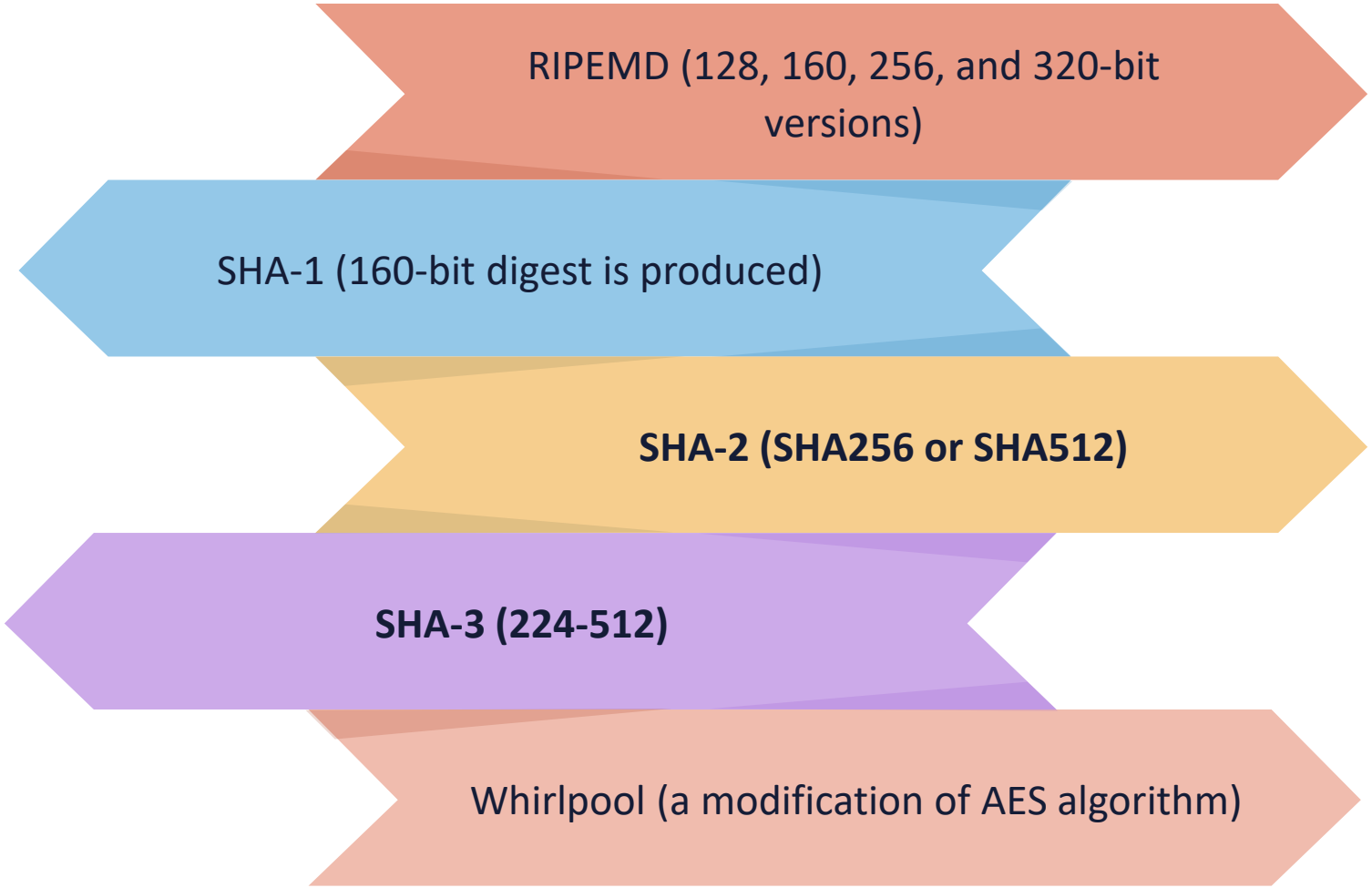
- Database encryption is the process of using an algorithm to transform data stored in a database into unreadable cipher text
- The purpose is to protect the data stored in various platforms from being accessed by external attackers or even compromised privileged insiders
- When using a cloud database service, key management services are often used
- Record encryption will encrypt and decrypt the individual records in a database systems

CRYPTOGRAPHIC HASHING



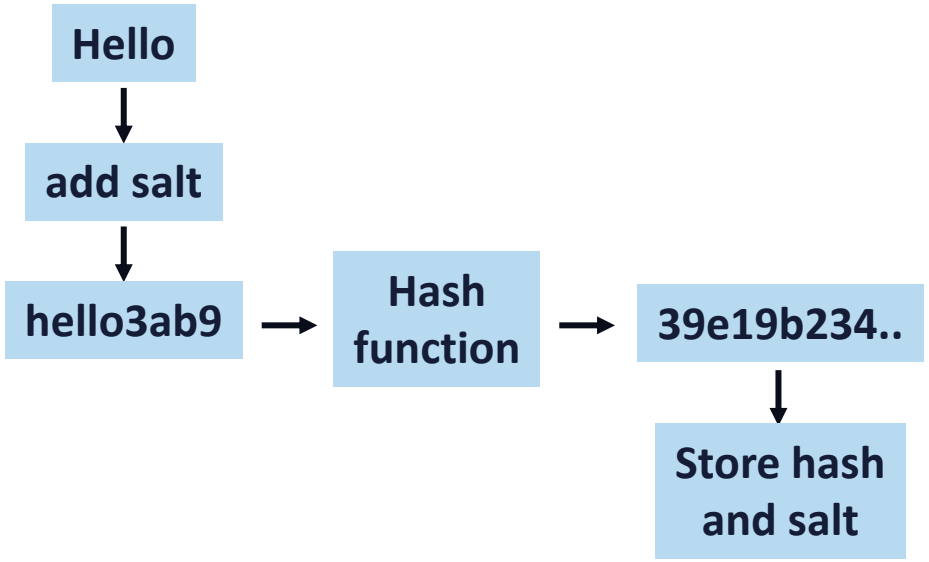
- A one-way mathematical function that produces a digest of 128 to 512 bit
- Converts data of any input size to a fixed-length string called a hash value, message digest, or fingerprint
- An advanced version of a simple checksum
- Birthday paradox, avalanche effect
- Used in authentication, data integrity, non-repudiation, fingerprinting, password storage, database indexing
- Must be collision resistant (no MD5)

COMMON HASH FUNCTIONS

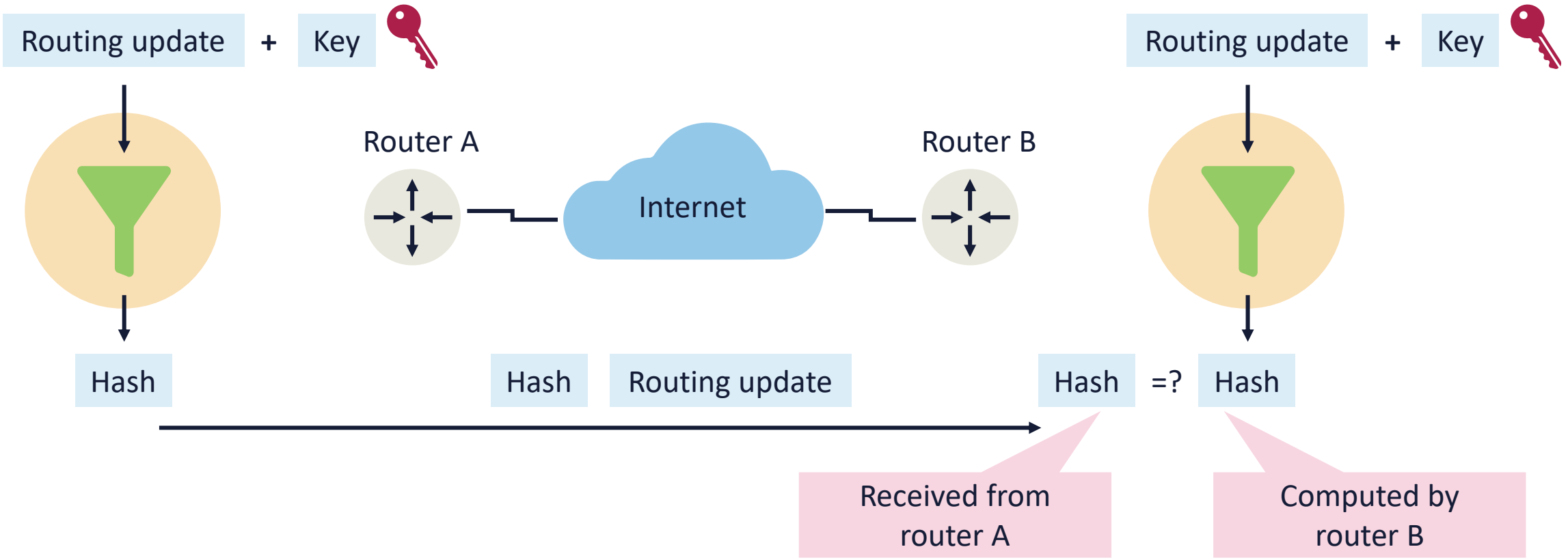


SALTING

- Salting is the technique of adding pseudorandom data to a cryptographic hash function
- The goal is to make it less deterministic for cracking tools
  - When an attacker can access a database of password hashes, they can use either hash tables or rainbow tables to look up matching hashes, which they can use to discover the passwords or other hashed data
- Two weaknesses are salts that are too short or if they aren't unique for each password



HASH-BASED MESSAGE AUTHENTICATION CODES (HMACS) FOR INTEGRITY AND ORIGIN AUTHENTICATION



KEY EXCHANGE

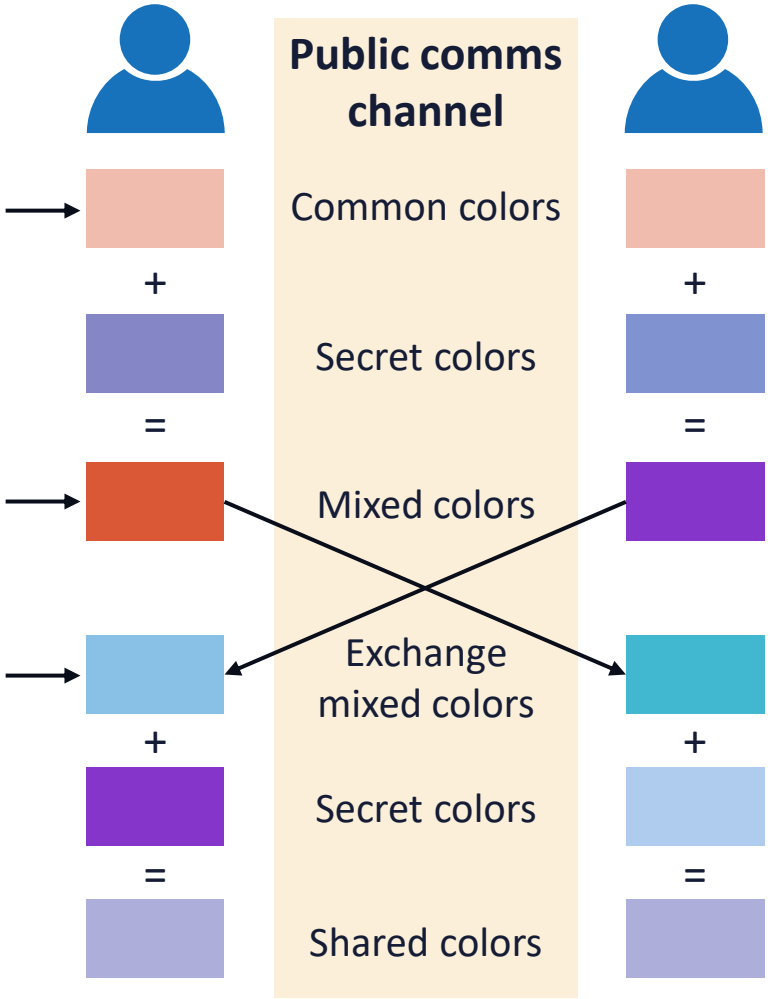
- There are several ways for parties to exchange keys:
  - Phone or text
  - Secured email
  - Couriers
  - Diplomatic bags
- Alternatively, a more effective method is using an asymmetric key exchange algorithm, such as:
  - RSA key exchange
  - Diffie-Hellman key exchange
  - Elliptic Curve Diffie-Hellman
  - Elliptic Curve Diffie-Hellman Ephemeral

DIFFIE-HELMAN KEY EXCHANGE

- Diffie-Hellman key exchange (DHKE) and RSA key transport are original protocols created for establishing secret keys between two parties over an unsecure channel
- Diffie-Helman is a widely used asymmetric cryptosystem found in SSH2, TLS, and IPsec
- It represents an impressive application of the discrete logarithm problem
- The RSA algorithm can sign public-key certificates, whereas the Diffie-Hellman key exchange cannot

BASIC CONCEPT OF DHKE

Note: Attacker only sees these colors and thus cannot arrive at the shared secret

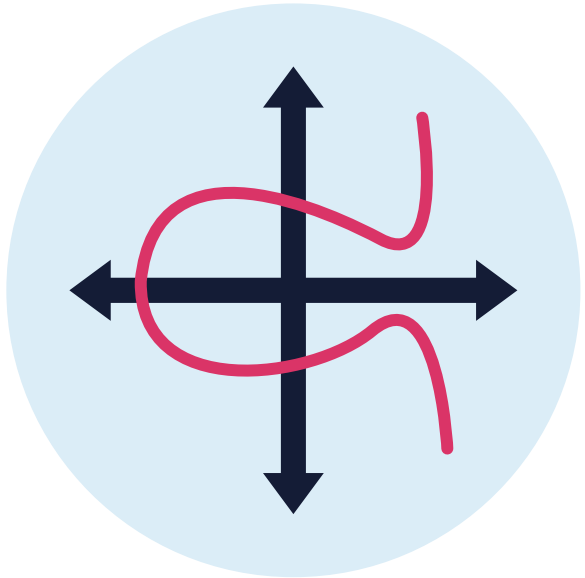


Note: Assume colors are hard to unmix, which means the secret colors are secure

DIFFIE-HELMAN MODES

- DH (Diffie-Hellman)
  - The same shared secret is used all the time between parties
- DHE/EDH (Ephemeral Diffie-Hellman)
  - A different shared secret is used each time between parties
- ECDH (Elliptic Curve Diffie-Hellman)
  - Uses EC public/private key pair
  - The same shared secret is used all the time between parties
- **ECDHE/ECEDH (Elliptic Curve Ephemeral Diffie-Hellman)**
  - Uses EC public/private key pair
  - A different shared secret is used each time

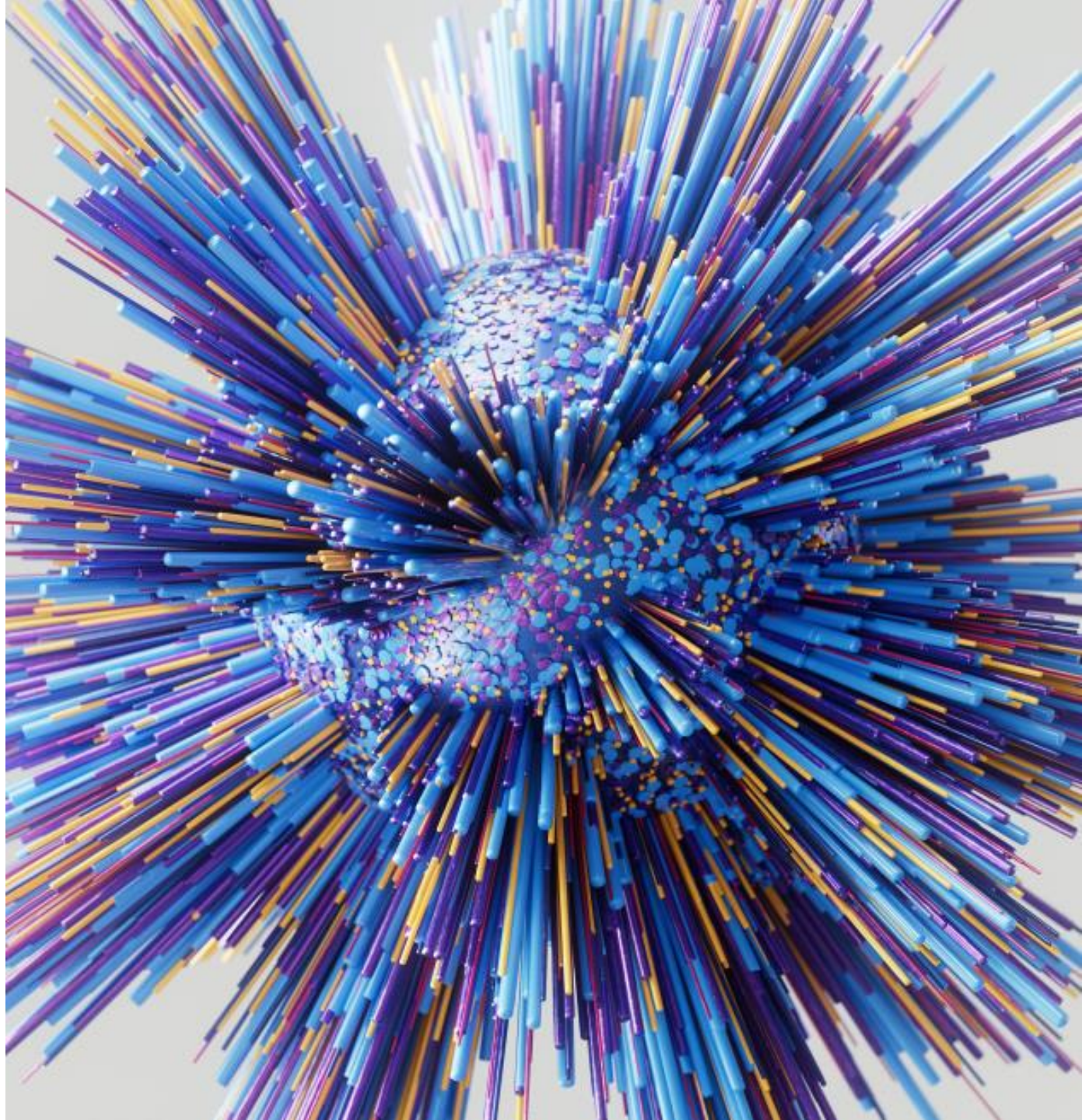
ECDHE/ECEDH (ELLIPTIC CURVE DIFFIE-HELLMAN EPHEMERAL)



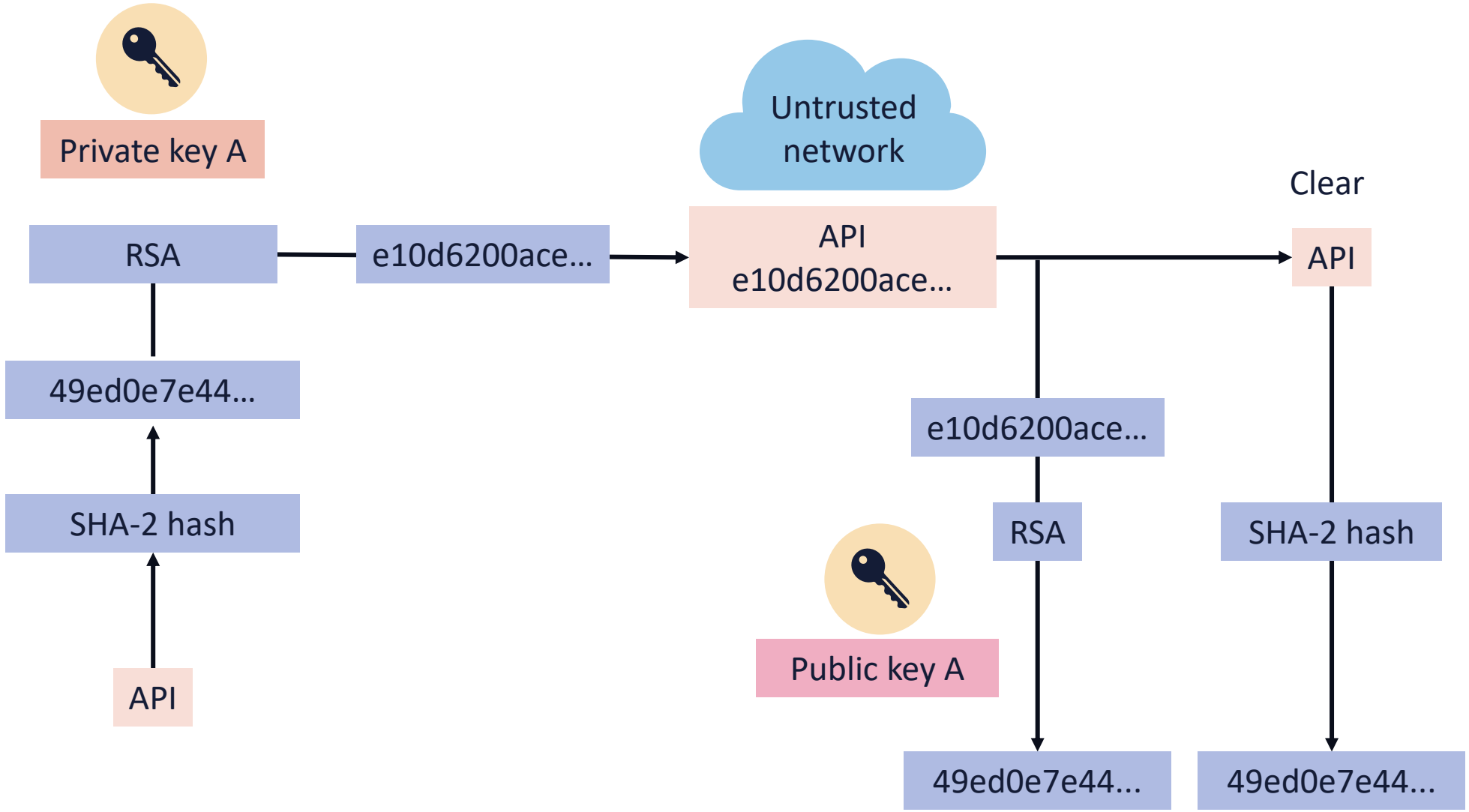
- Based on rich math functions of values plotted on an elliptic curve
- Uses smaller keyspaces while offering superior strength
- 256-bit elliptic key = 3072-bit standard key
- Excellent for mobile devices and IoT with limited memory and processing power
- Common use cases:
  - Key exchange
  - IPsec and TLS
  - Digital signatures

DIGITAL SIGNATURES

- These are a scalable mechanism for providing authenticity, integrity, and non-repudiation using random public/private key pairs
  - Does not offer confidentiality
- Digital signatures are legally equivalent to a handwritten signature in many countries
- SHA1/2/3 hash algorithms are commonly used
- Signing algorithms:
  - Rivest-Shamir-Adelman (RSA)
  - Digital Signature Algorithm (DSA)
  - Elliptic Curve Digital Signature Algorithm (ECDSA)



DIGITALLY SIGNING AN API CALL



DIGITAL CERTIFICATES

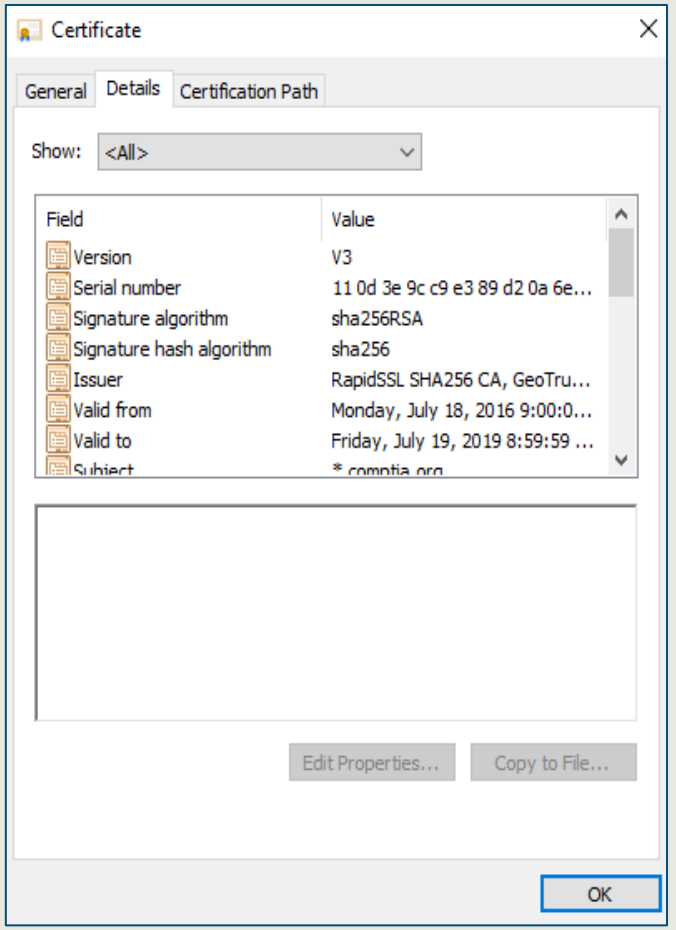
- A digital certificate is a form of file used to bind cryptographic key pairs to entities such as individuals, websites, devices, or organizations
- If validity affirmation and/or public trust is needed, then a trusted certificate authority (CA) will assume the role of a third party to validate, identify, and associate them with cryptographic pairs using the digital certificates

DIGITAL CERTIFICATES

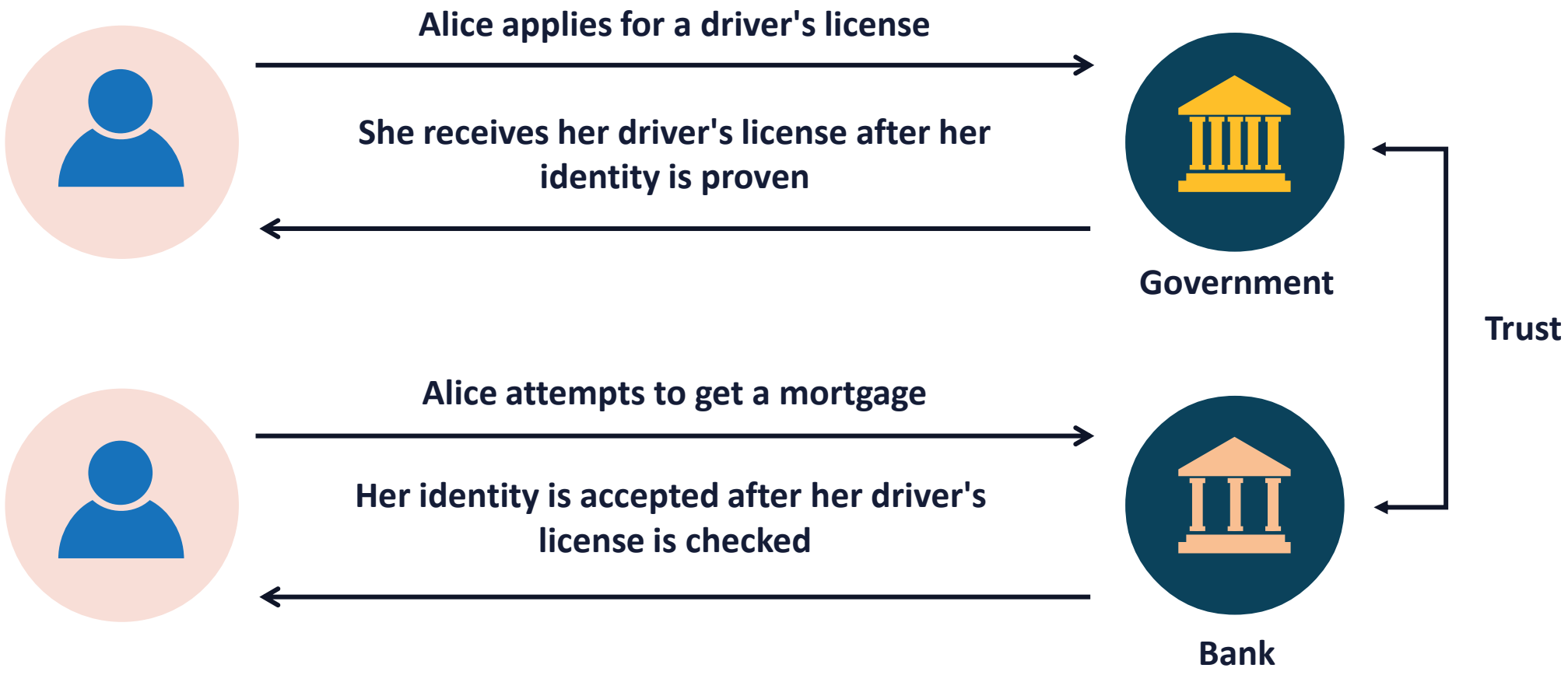
- The key pair consists of a public key and a private key
- The public key is included in the certificate, while the private key is stored in a secure fashion
- The owner of the private key can then use it to sign documents, and the public key can be used to verify the validity of those signatures
- A common format for digital certificates is based on the X.509 standard

X.509V3 DIGITAL CERTIFICATES

- Version number
- Serial number
- Signature algorithm ID
- Issuer name
- Validity period
- Not before
- Not after
- Subject name*
- Subject alternative name (SAN)
- Subject public key info
- Public key algorithm
- Subject public key
- Issuer unique identifier
- Subject unique identifier
- Extensions
- Certificate signature algorithm
- Certificate signature

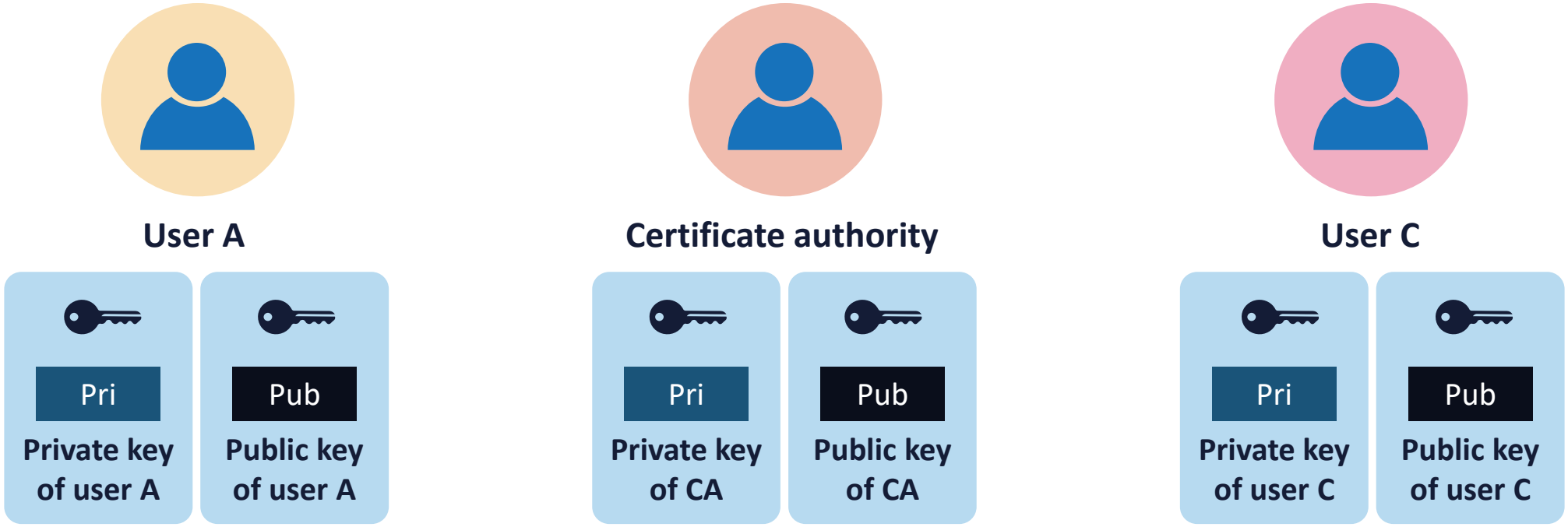


TRUSTED THIRD PARTIES



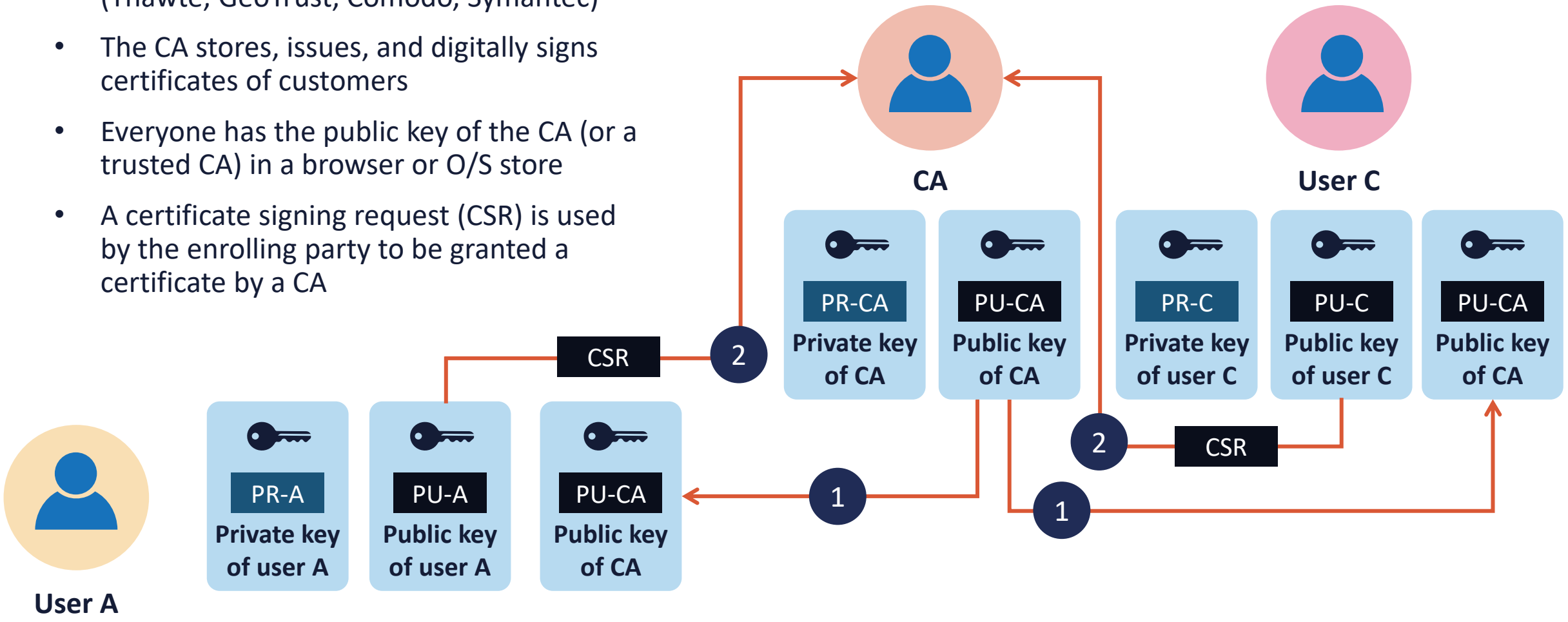
PUBLIC KEY INFRASTRUCTURE (PKI)

- PKI is a scalable binding of a public key with an entity identity
  - A person, system, or organization
- Digital certificates are registered and issued by a certificate authority (CA)
  - Can be automated or manual
- The CA may also generate the key pair (usually RSA) for the requesting party



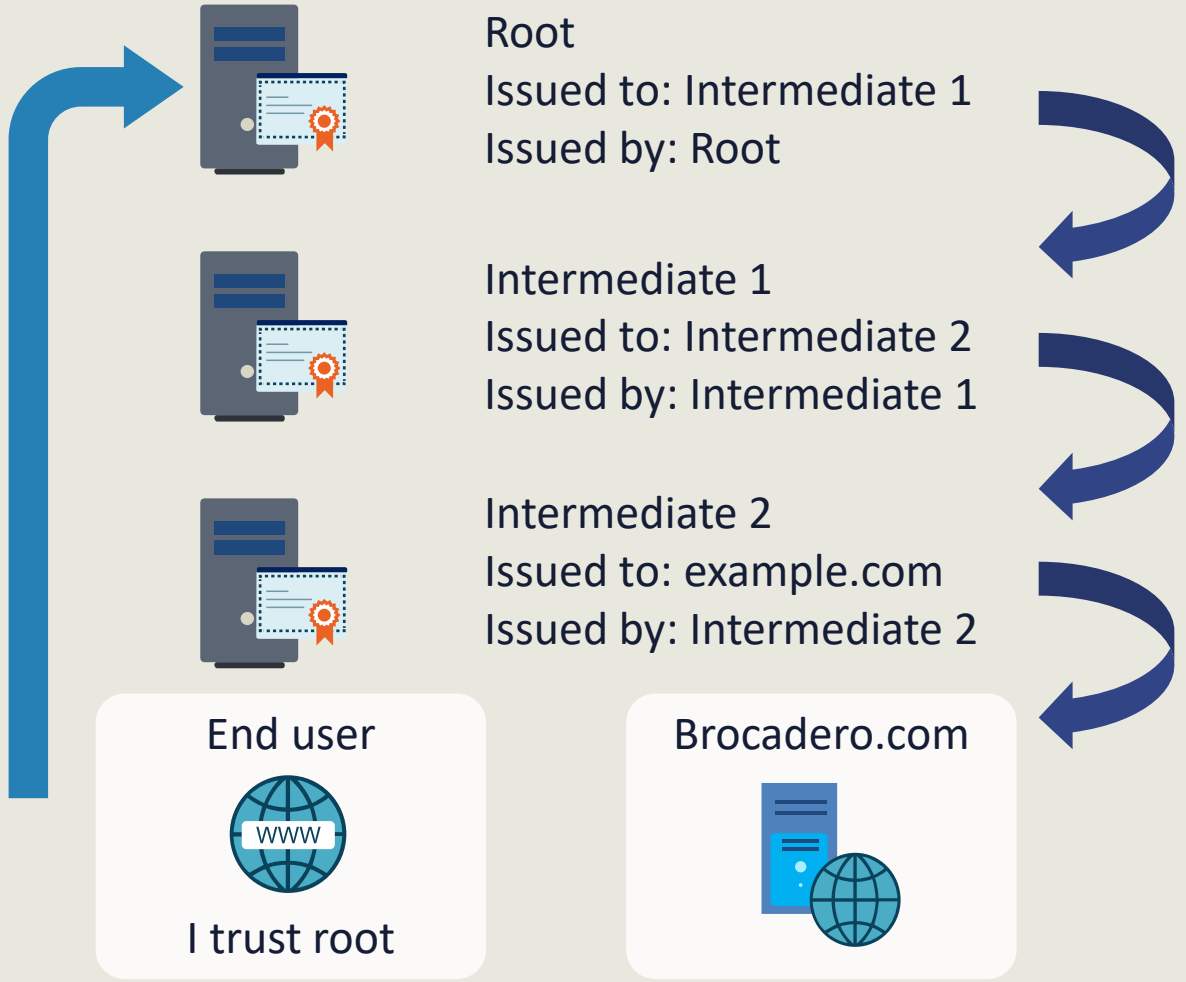
PUBLIC KEY INFRASTRUCTURE (PKI)

- The CA is the central trusted introducer (Thawte, GeoTrust, Comodo, Symantec)
- The CA stores, issues, and digitally signs certificates of customers
- Everyone has the public key of the CA (or a trusted CA) in a browser or O/S store
- A certificate signing request (CSR) is used by the enrolling party to be granted a certificate by a CA



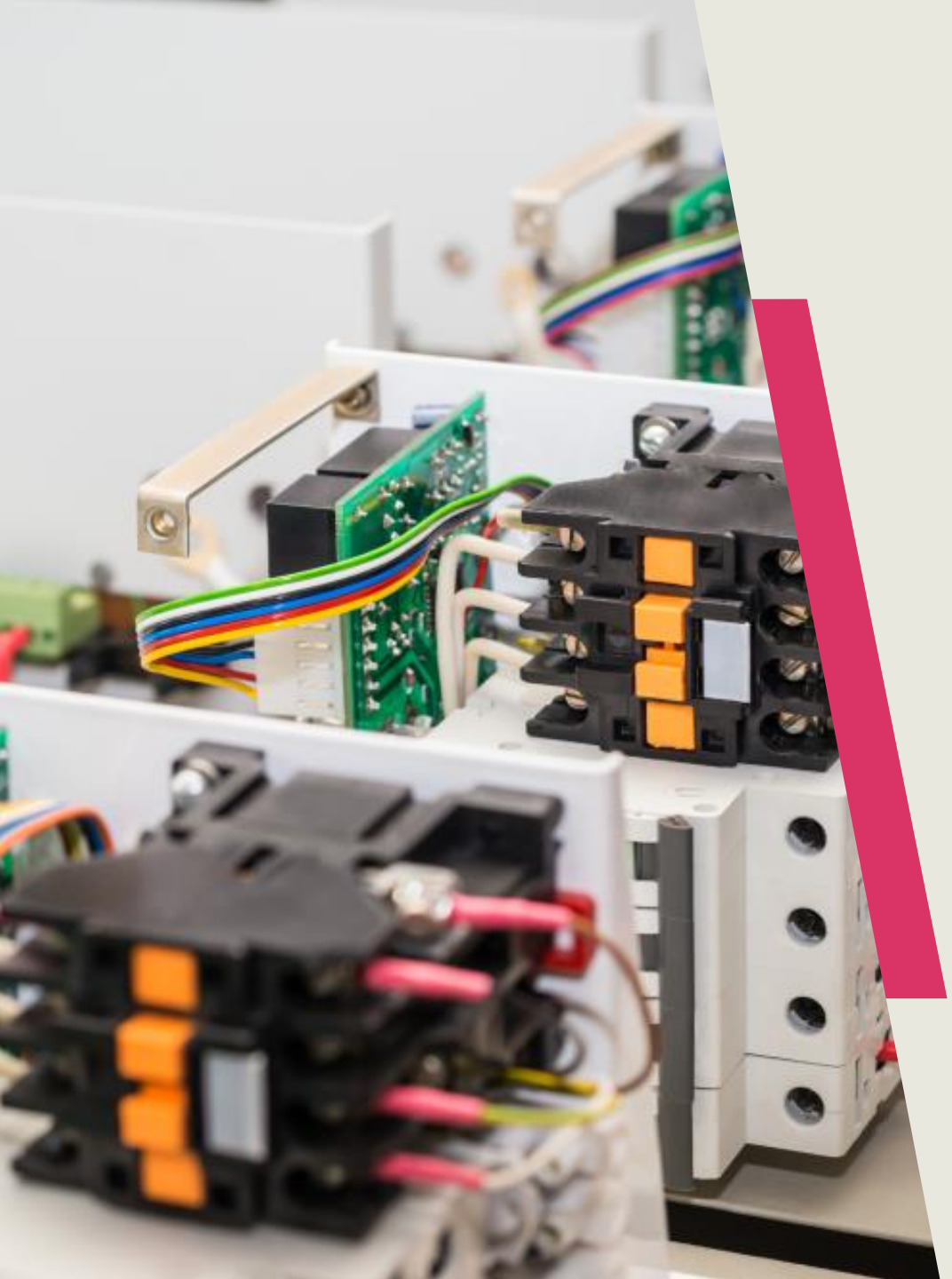
CA TRUST MODELS

- Single CA:
  - Responsible for directly providing certificates to everyone (enterprise PKI)
  - Must always be online
- Hierarchical CA:
  - Combination of root CA and intermediate CAs
  - Root sends certificates to intermediates
  - Intermediate CAs provide certificates and the "chain" to users or other intermediate CAs
  - Root can be online or offline
- Online – connected to the network and issues certificates over the network
- Offline – not connected to the network and issues certificates on removable media



CERTIFICATE REVOCATION AND SUSPENSION

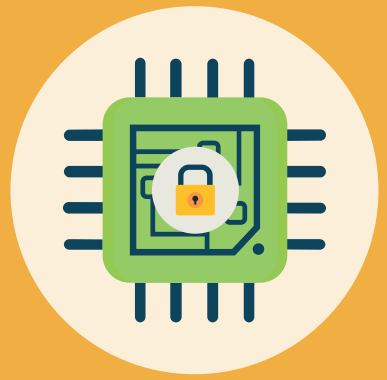
- Certificates are stamped with non-deterministic serial numbers and validity dates
- For security reasons, all keys must have a finite life due to brute-force attacks
- Certificate can be
  - Revoked (permanent) – never used again
  - Suspended/held (temporary) – can be reactivated
- The certificate revocation list (CRL) is the original method for revoking certificates
- Online Certificate Status Protocol (OCSP) is an Internet-enabled transactional database that CA's and web servers utilize for suspension and revocation



TRUSTED PLATFORM MODULES (TPM)

- A TPM is used to improve the security of various systems, such as servers and PCs
- Microsoft uses services like BitLocker Drive Encryption, Windows Hello, and others to securely create and store cryptographic keys
- It is often a separate chip on the motherboard (TPM 2.0) that allows manufacturers to build the capability into their chipsets rather than requiring a separate chip
- Google employees store X.509v3 certificates in TPMs in devices as part of zero trust

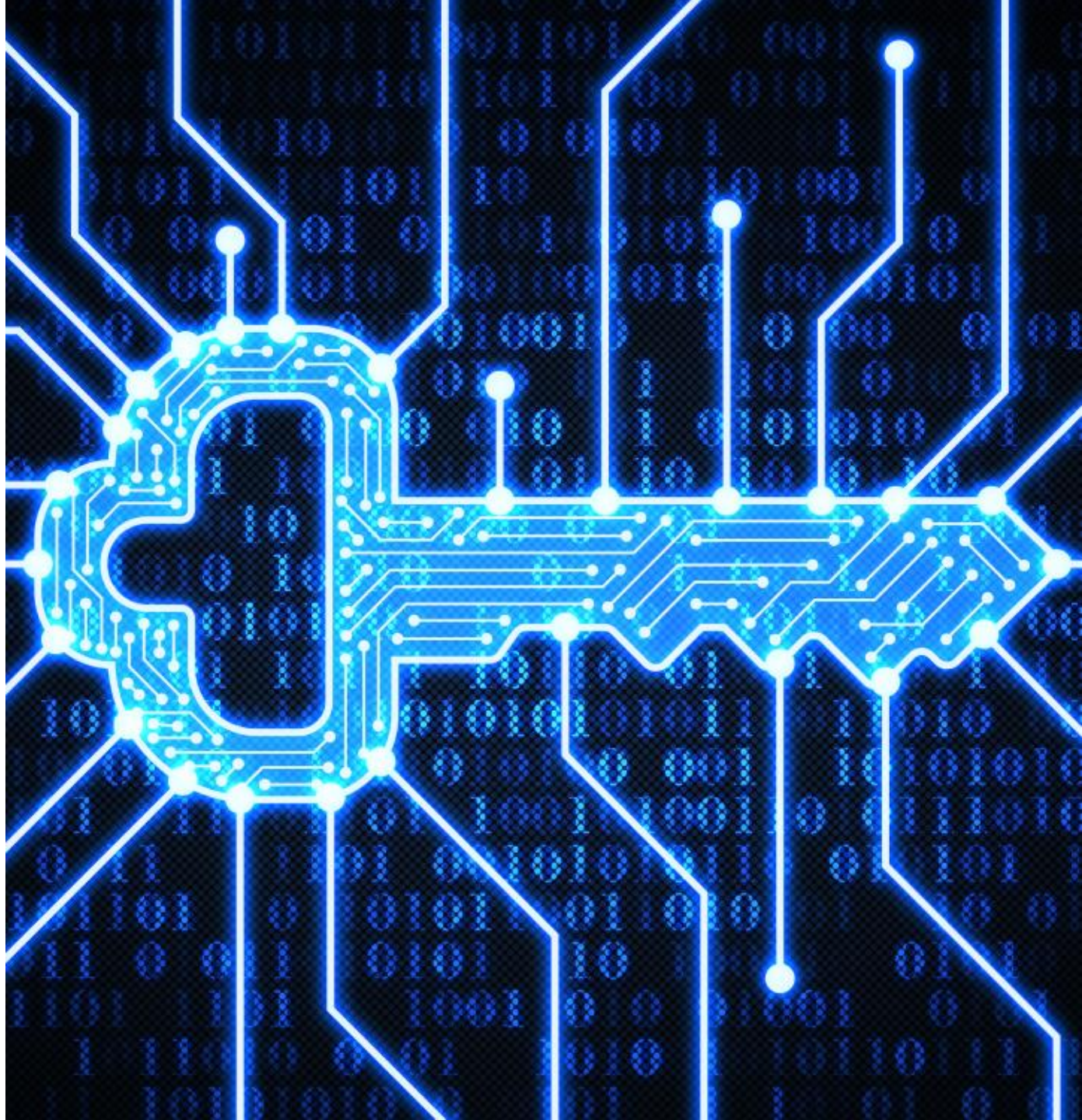
HARDWARE SECURITY MODULES (HSMs)



- These are hardened, tamper-resistant dedicated appliances or integrated modules in a PC/server
  - HSMs can be physical or virtualized
- A SmartCard-HSM is a lightweight hardware security module in a smart card, MicroSD, or USB form factor providing a remotely manageable secure RSA and ECC keys
- Responsibilities include:
  - Managing, processing, generating, and storing keys
  - Verifying digital certificates
  - SSL connection accelerator
  - Encrypting sensitive data
  - Verifying the integrity of stored data

KEY MANAGEMENT SERVICES

- A cloud-based key management service (such as AWS KMS) is a managed service that enables the creation and control of customer-managed symmetric and asymmetric cryptographic keys to protect various types of data at rest
- These key services integrate with many other cloud services, such as block storage, object (blob) storage, applications, and databases to facilitate the encryption of critical data

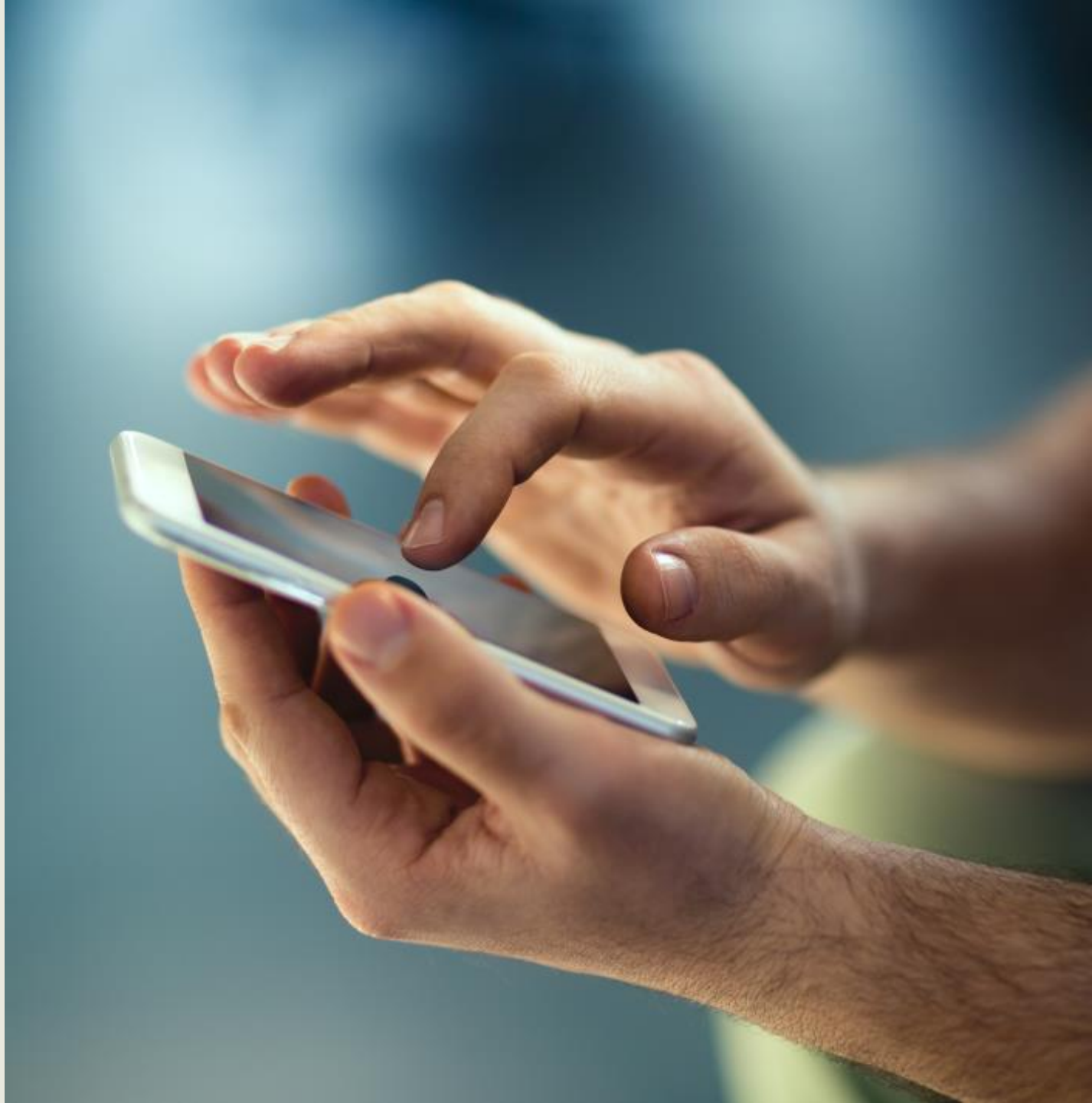


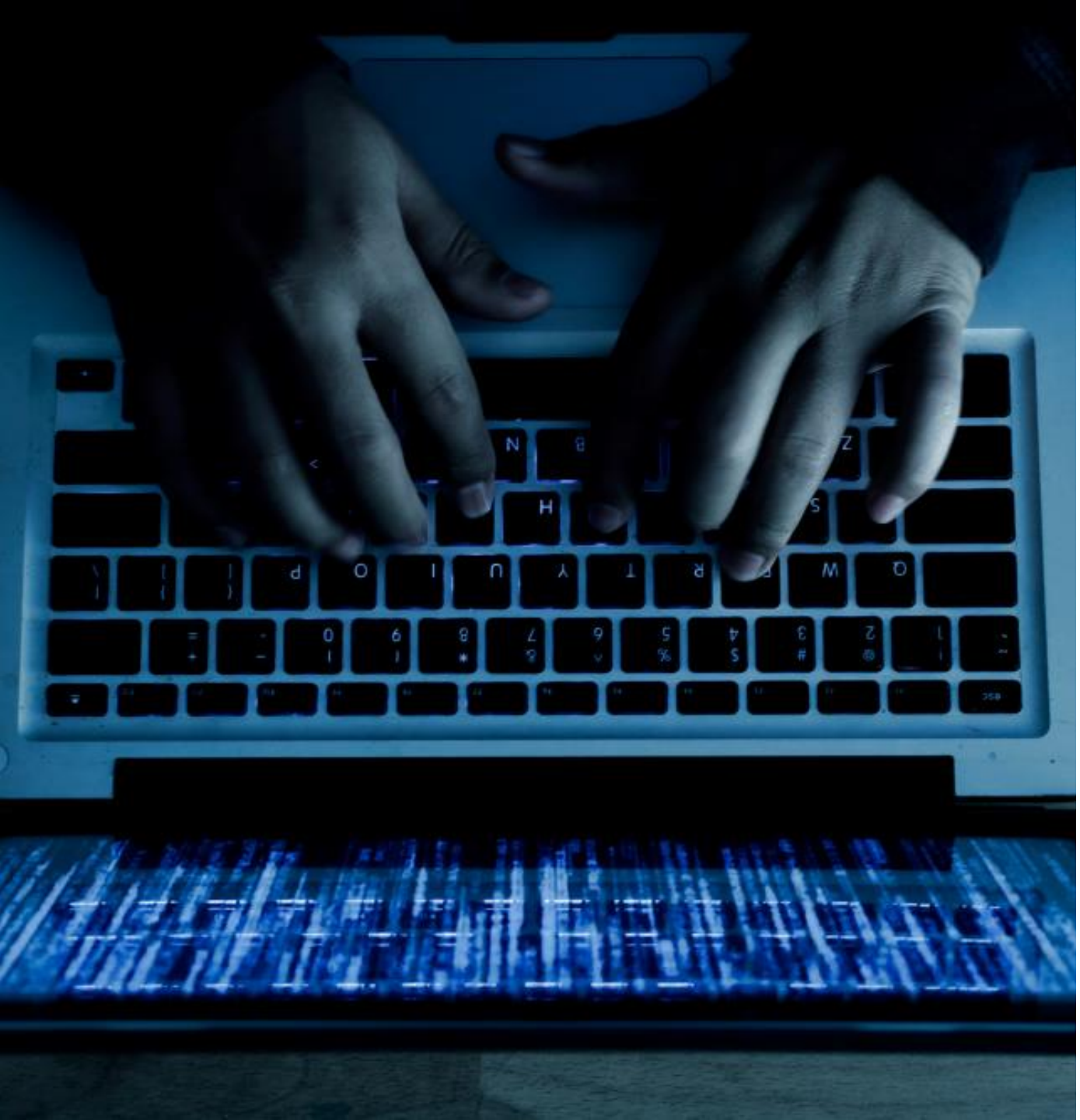
KEY STRETCHING

- Tools such as PBKDF2 apply a pseudorandom function, such as an HMAC, to the input password or passphrase along with a salt value
- PBKDF2 then repeats the process many times (1000 iterations) to produce a derived key, which can then be used as a cryptographic key in further operations
- The stretching process makes password cracking much more difficult
- Today, programs will use hundreds of thousands of iterations due to fast processors

SECURE ENCLAVES

- A secure enclave delivers CPU hardware-level isolation and memory encryption on a server, workstation, or mobile device by isolating application code and data from anyone with privileges and encrypting its memory
- With additional software, Secure Enclaves enable the encryption of both storage and network data for simple full-stack security
- Secure enclave hardware support is built into all new CPUs from Intel and AMD
- The Secure Enclave is a hardware feature of most versions of iPhone, iPad, Mac, Apple TV, and Apple Watch





STEGANOGRAPHY

- Steganography is the process of hiding a secret message inside of (or even on top of) something that is not secret
- Tools like Steghide often involve embedding a secret piece of text inside of a picture or hiding a secret message or script inside of a Word, Excel, or PDF document
- It is a form of covert communication but not a form of cryptography because it doesn’t involve scrambling data or using a key
- Steganography is a practice that enables secrecy and deceit

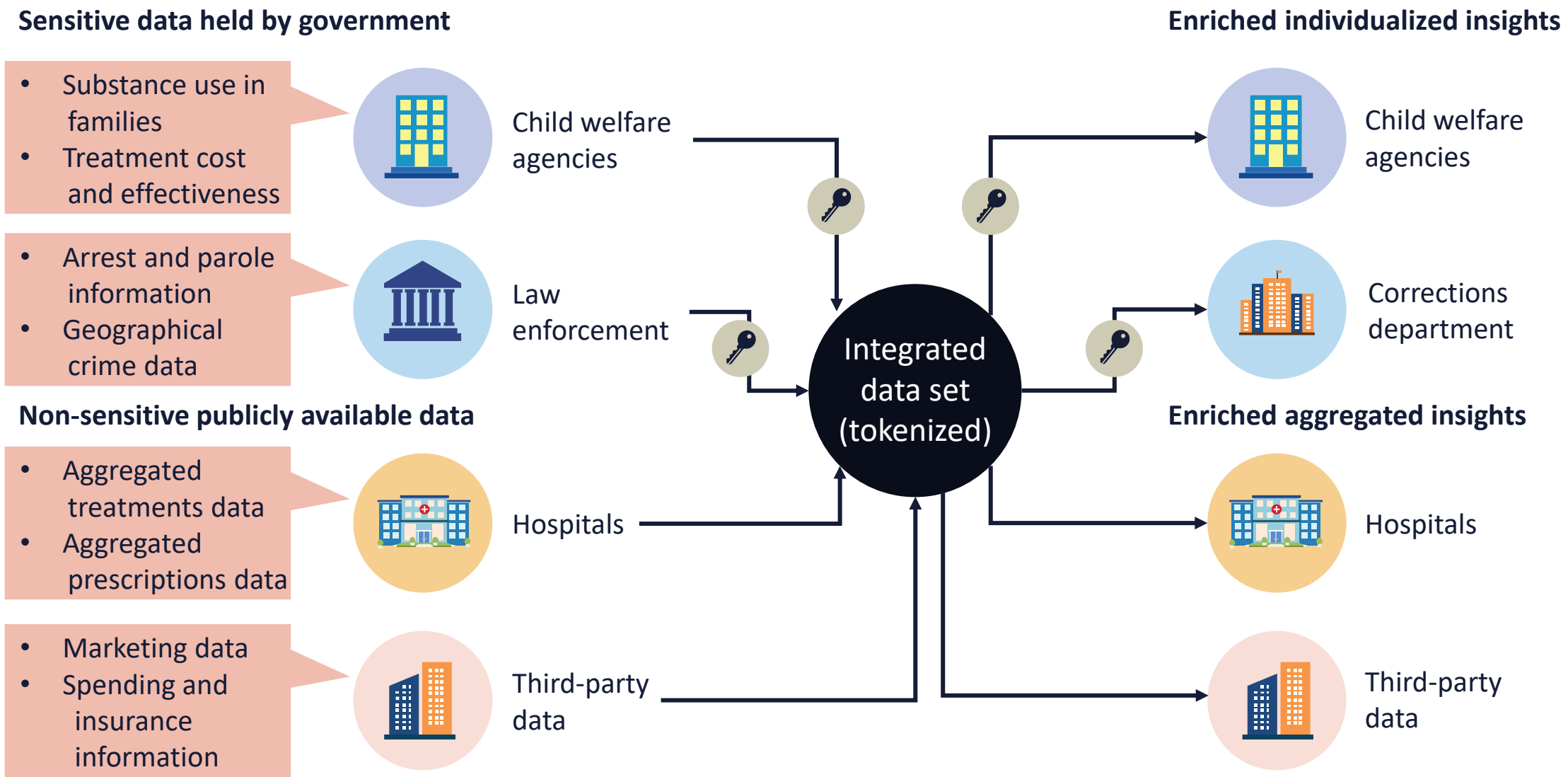
DATA MASKING

- Masking often involves using characters like "X" to hide some or all data
- For example, only displaying the last four digits of:
  - Social Security numbers
  - Credit card numbers
  - National ID numbers
  - Bank account numbers
  - Usernames or email addresses
- Methods to obfuscate data should prevent inference, and therefore, masking is suboptimal when compared to other methods like tokenization

TOKENIZATION

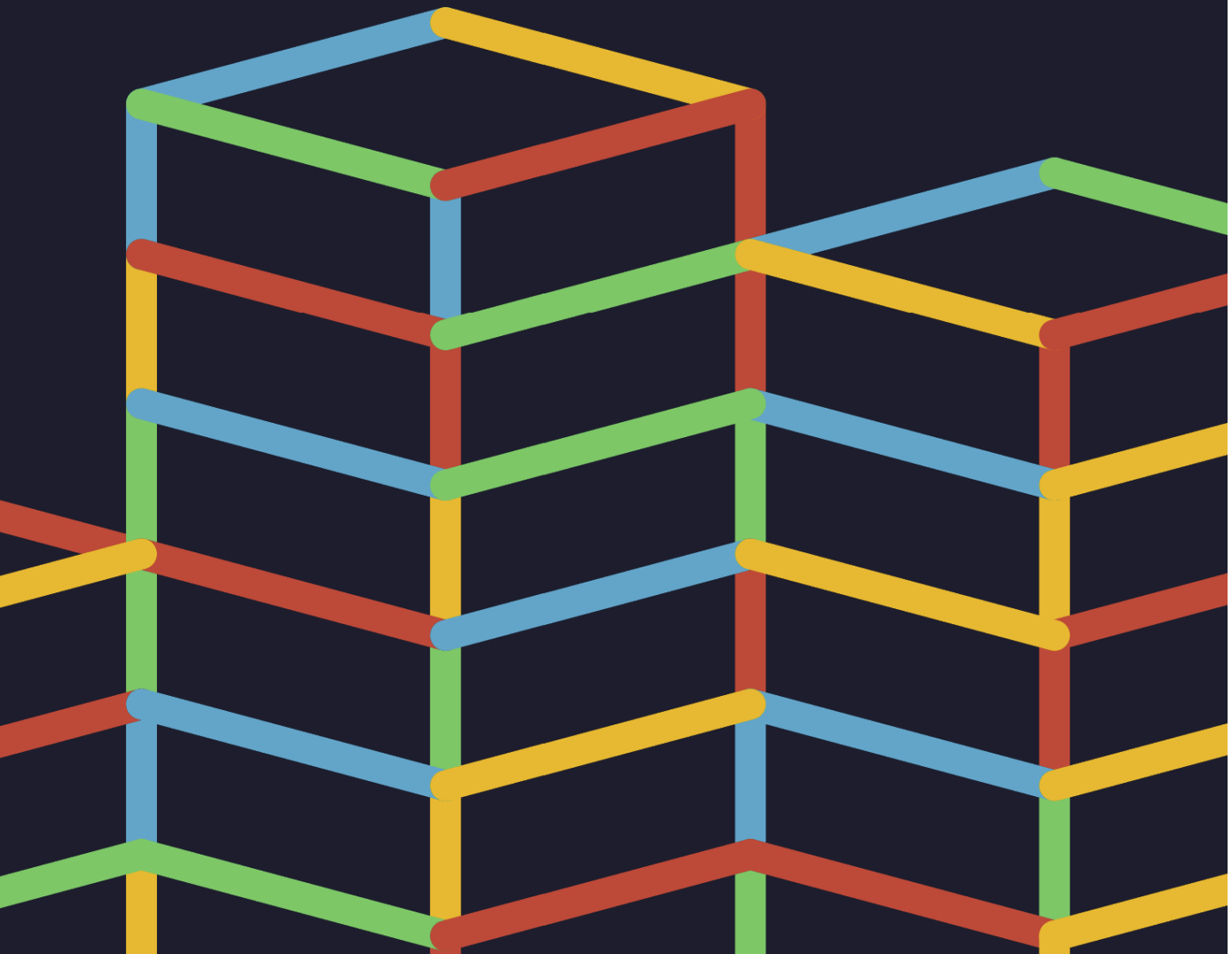
- Tokenization involves sending sensitive data through an API call (or batch file) to a provider that replaces the data with non-sensitive placeholders called tokens
- The practice involves two distinct databases:
  - One with the actual sensitive data
  - One with tokens mapped to each chunk of data
- Unlike encrypted data, tokenized data is irreversible and unintelligible

TOKENIZATION EXAMPLE



BLOCKCHAIN TECHNOLOGY

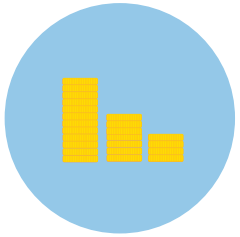
- A blockchain is a distributed database that leverages a constantly growing list of ordered records called blocks
- These blocks are linked using cryptographic mechanisms
- Each block stores a cryptographic hash of the previous block, a timestamp, and transaction data
- Blockchain may be deployed as a public ledger (or private smart contract) consisting of a digital "chain of blocks" storing information



BLOCKCHAIN TECHNOLOGY

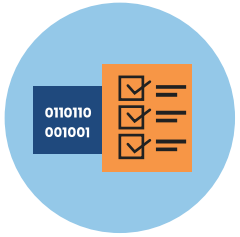
- Data can be read or written to the chain but not modified (immutability) – changes must be made to a subsequent block in the chain
- Transaction data such as date, time, and amount is verified with a consensus mechanism (proof of work [PoW], proof of stake [PoS], etc.)
- The transaction participant's identities are based on digital signatures
- Unique cryptographic hashes are used to distinguish the blocks from each other

BLOCKCHAIN USE CASES

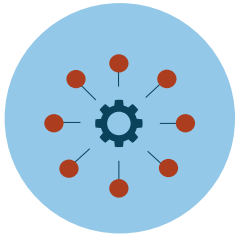


Cybercurrencies and tokens

Money and asset transfer ledgers



Smart contracts



Non-fungible tokens (NFTs)

Government services

Insurance claims (fraud prevention)

Securities (stocks, bonds)

Healthcare