SOS CHAIN

Advanced Security for Data and People

You can **now** activate your
Unified Health ID,
receive **notifications** to keep your
Unified Health Index up-to-date,
share **digital twins** for research,
request assistance and **be located** in **emergencies**
via SMS and **Bluetooth** devices.

SOS CHAIN

SOS CHAIN

A new paradigm:
*the Unified Health ID**

Experience the impact of creating
your own **worldwide Unified Health ID***
to **be attended** to by emergency services and
clinicians **anywhere**.

*Patent US 11,636,776

Collaborative
Shared Data Space

Use a secure bridge to **receive notifications** from patient portals to your **Unified Health ID***, enabling your Unified Health Index: **Have your data ready, anytime!**

*Patent US 11,636,776

SOS CHAIN

Real-time healthcare data updates

Your Unified Health Index works like **a book index**, **automatically updating** links to new pages in different sections, sent from distinct patient portals **to your Unified Health ID*** or associated IDs.
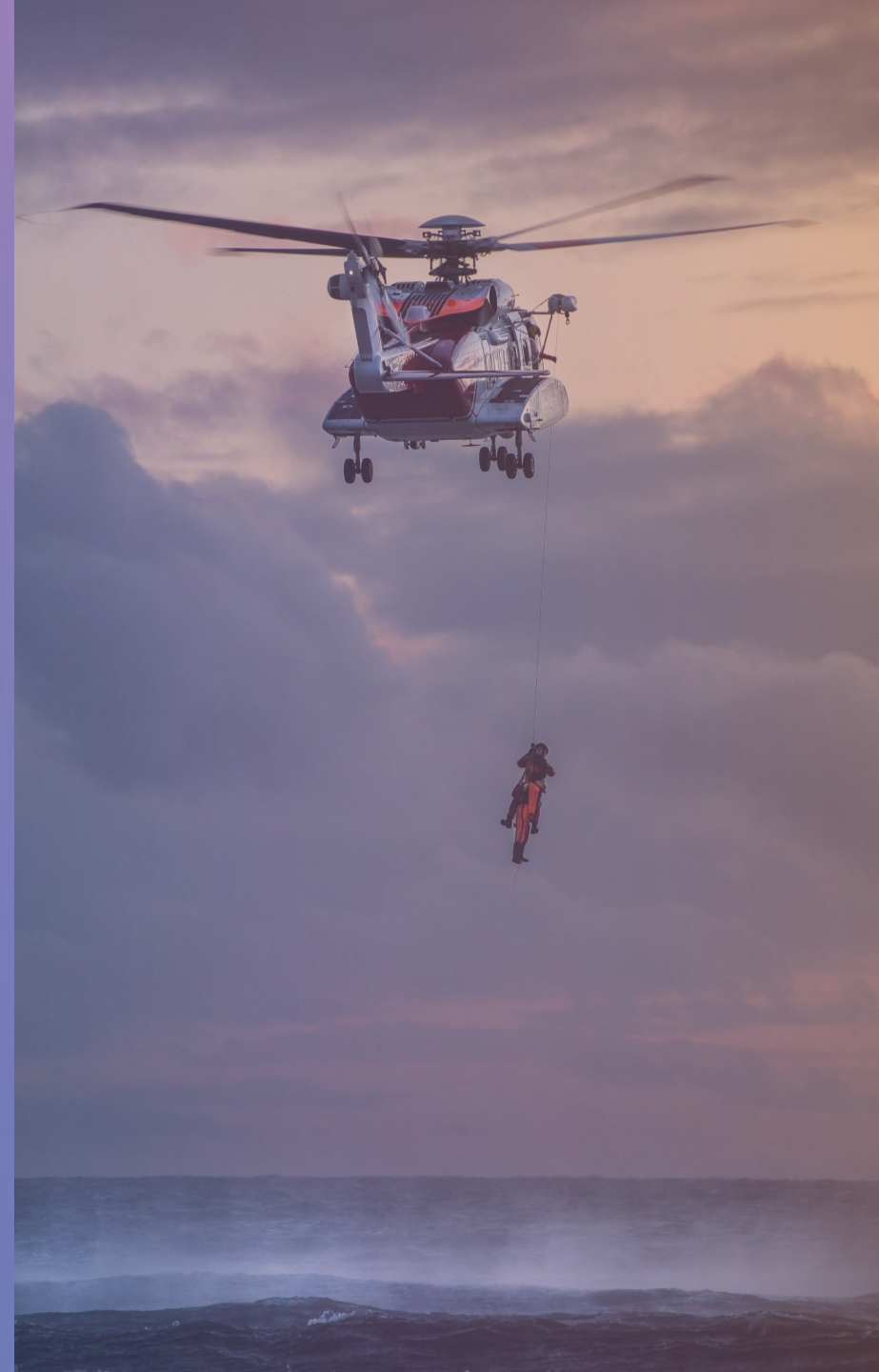
*Patent US 11,636,776

Associate your *Identifiers and Devices*

Link **any other identifier or device****
to your Unified Health ID*.
Authorize being located by rescue services
via location devices** (Bluetooth or others)
in **emergency situations**.

*Patent US 11,636,776
**QuantumPrime is used for generating anonym device identifiers (digital twin).

Receive Trusted Data
and
Request Assistance

Get **notifications and information**
from **trusted sources** (to avoid fake news).
Send **service requests to emergency services**
including your **Unified Health ID***, device ID**,
severity and type of emergency.

*Patent US 11,636,776
**QuantumPrime is used for generating anonym device identifiers (digital twin).

Unified Health Index: create your International Health Booklet

SOS CHAIN

A **new paradigm**:

- Create your Unified Health ID*
- Associate other identifiers
- Enable your Unified Health Index
- Receive notifications about your data!

*Patent US 11,636,776

1 **Sign your consent** to create your international, **Unified Health ID***

2 **Receive updates** in your **Unified Health Index** automatically: URL and the section it belongs to

3 **Retrieve your data** to construct your **International Patient Summary (IPS)** and assign **permissions**

4 **Easily anonymize** your data to create your **Digital Twin** and securely share it **for research**
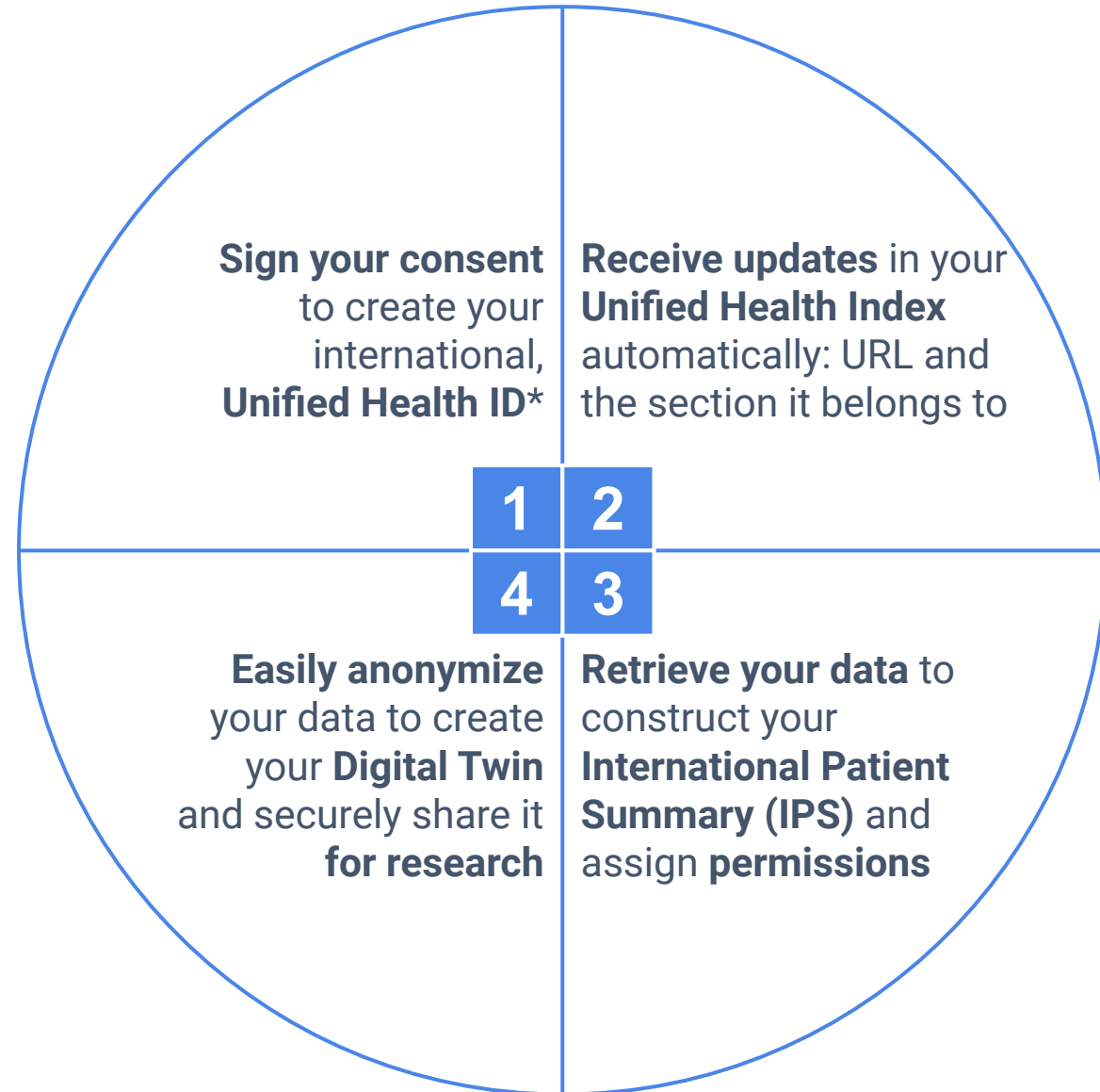
Registering organizations and employee roles on Blockchain

SOS CHAIN

The **fundamental data communication tool***

- **Prevent fraud**: verified identities and messages
- **Optimize time** in medical consultations
- **Reduce diagnostic errors** and **readmissions**
- Secure data and messages: post-quantum algorithms

Patent US 11,636,776

1 **Request to register** the organization with a **signed consent**

2 **Receive** the **Activation Code** upon verification to get started: create employees and roles

3 **Obtain permissions** from patients or legal guardians to **gain a 360-degree, holistic view** for improving diagnosis and care

4 Obtain **digital twins** to **enhance AI** tools, **personalize medicine**, and **reduce healthcare costs**

SOS CHAIN

Blockchain: **public notary for security and trust***

- **Secure certification** of data and consents

- **Permissions** based on consents

- **Automation**: auditable and secure records

- Reduces administrative burden and operational costs

Patent US 11,636,776

Consent registration on blockchain with **digital certificate**

Verified digital identities using official digital certificates or through facilities

1 **2**

4 **3**

Optimize processes and costs through **automation** and **analysis** of **digital twins** (AI)

Grant or deny access permissions based on consents registered on blockchain
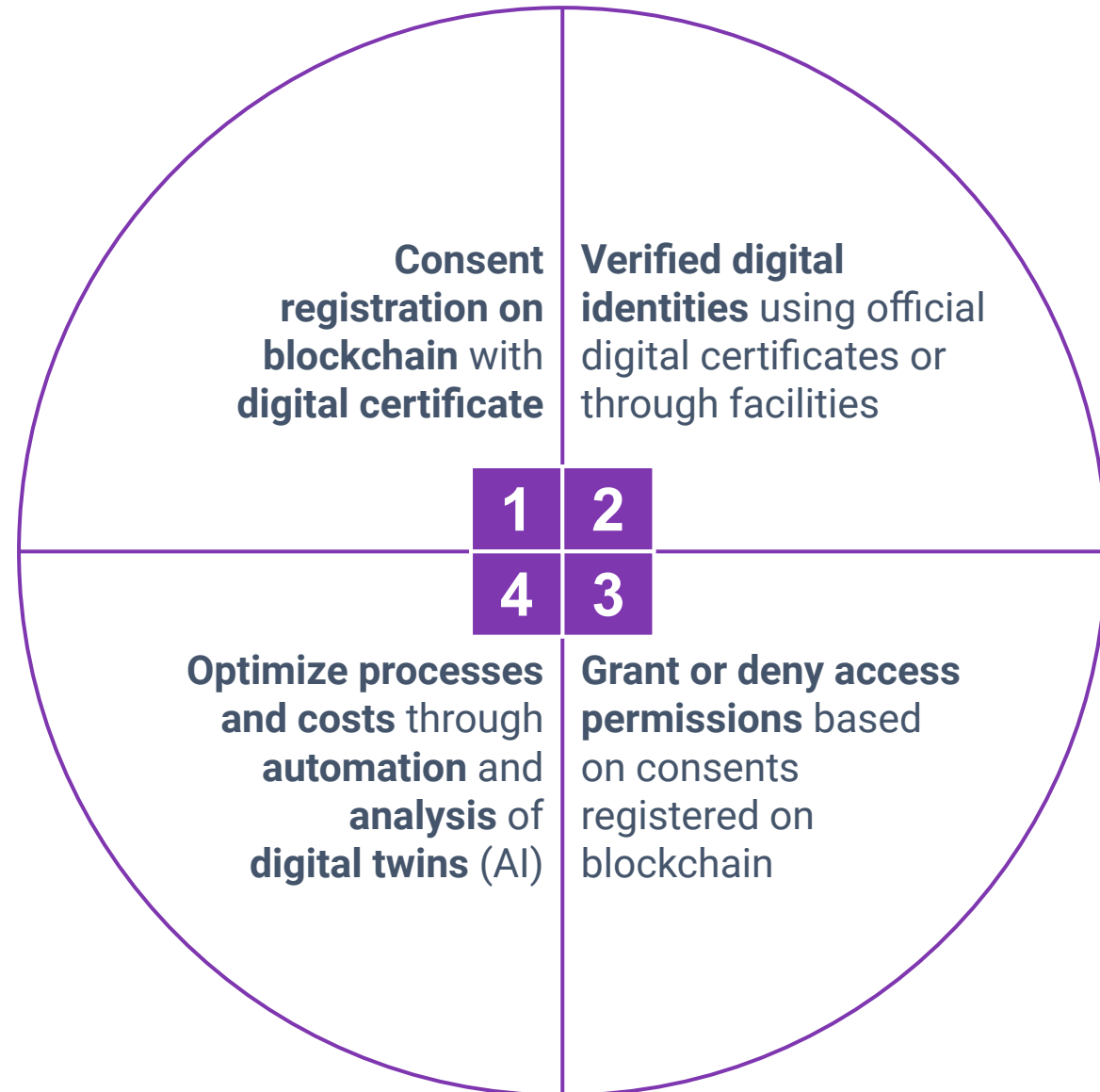
Localization in emergencies and rescues

SOS CHAIN

Devices and permissions for **emergency cases**:

- **Rescue request via SMS**: Unified Health ID*, device ID, coordinates, type of emergency, etc.

- **Localization** via Bluetooth devices and others: disoriented individuals, natural disasters, etc.

- **Access to contacts and data for emergencies**: allergies (e.g., penicillin, latex), pacemakers, etc

*Patent US 11,636,776

1 **Associate** your **Unified Health ID*** **with devices:** bluetooth, NFC, and others

2 **Authorize** being **located in emergencies** through the **device ID**

3 **Associate** the license **plate of the vehicle you are traveling in** or **your home** with your **Unified Health ID***

4 **Emergency and rescue services** will be able to **locate you** and **access data in emergencies**
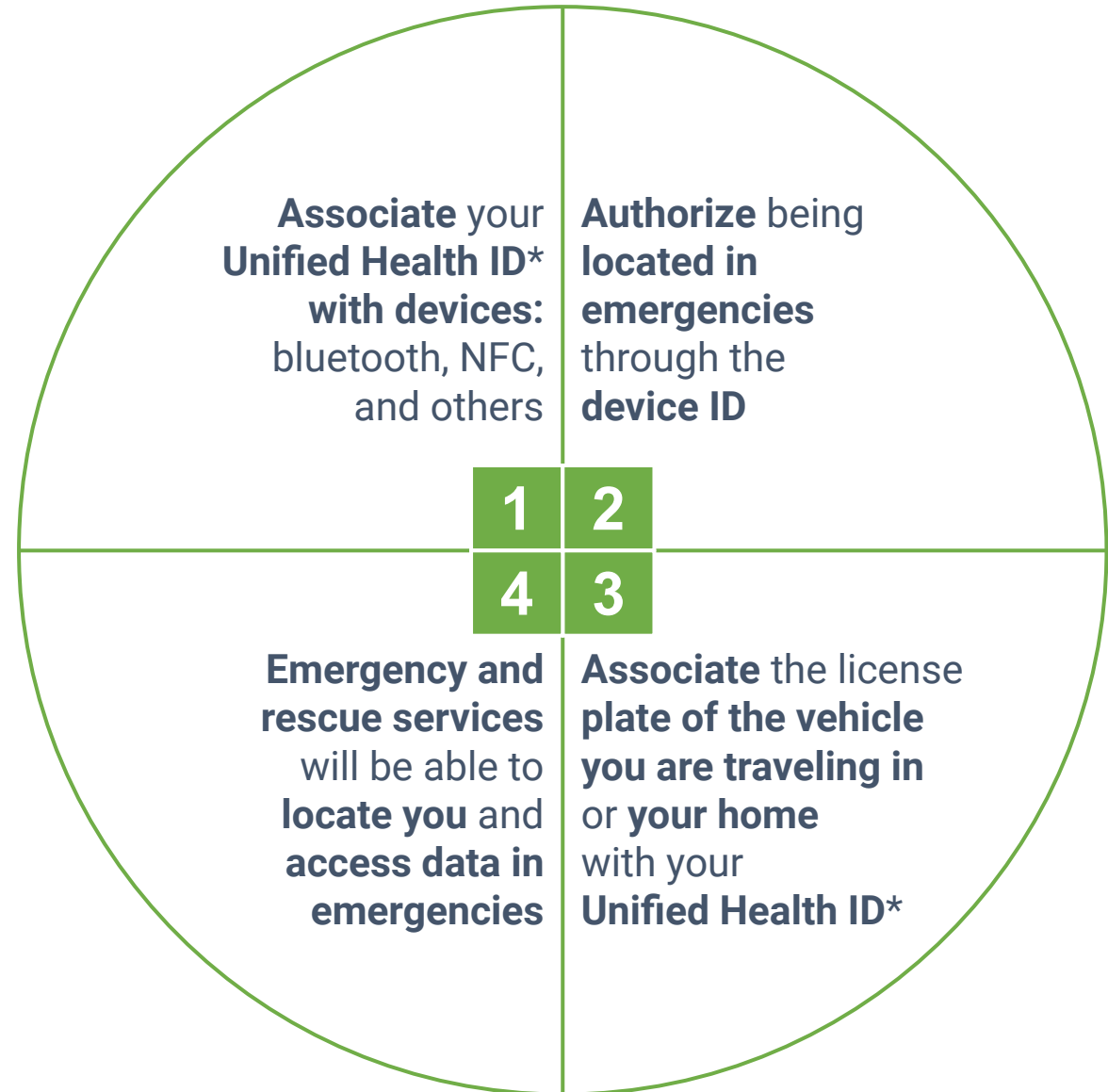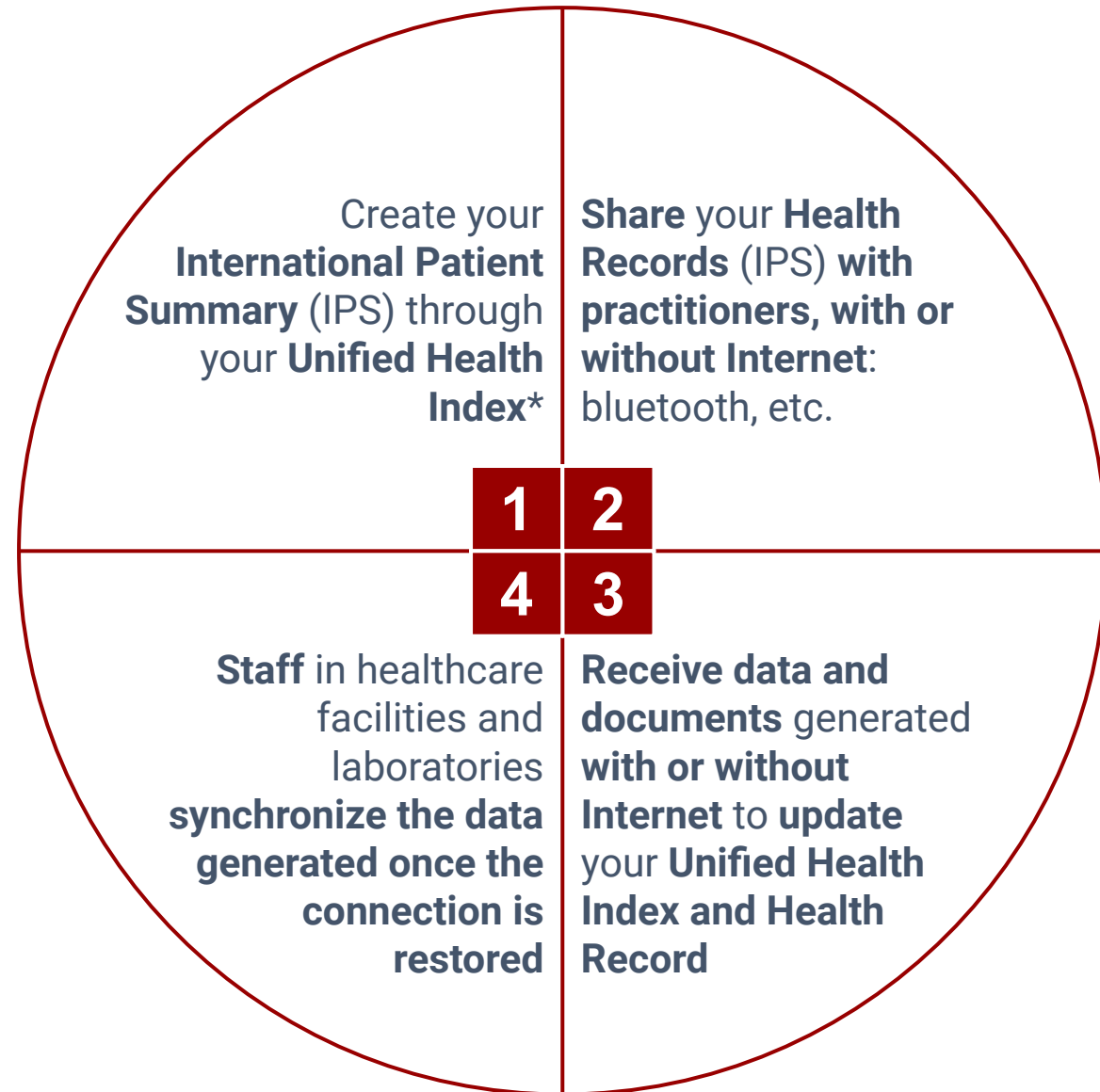
Improve resilience against system failures and attacks

SOS CHAIN

Create **cyber-resilient health ecosystems** as a **key and strategic sector** for the defense of countries.

- **Resilience**: The patient creates their International Health Record and shares it with medical services even without the Internet, using Bluetooth, etc.

- **Protection against disruptions**: Healthcare professionals create new documents and share them via Bluetooth, printed QR codes, or other means.

- **Recovery**: Patients and professionals synchronize the data once the connection is restored.

Patent US 11,636,776

1 Create your **International Patient Summary** (IPS) through your **Unified Health Index***

2 **Share** your **Health Records** (IPS) **with practitioners, with or without Internet**: bluetooth, etc.

4 **Staff** in healthcare facilities and laboratories **synchronize the data generated once the connection is restored**

3 **Receive data and documents** generated **with or without Internet** to **update** your **Unified Health Index and Health Record**

SOS CHAIN
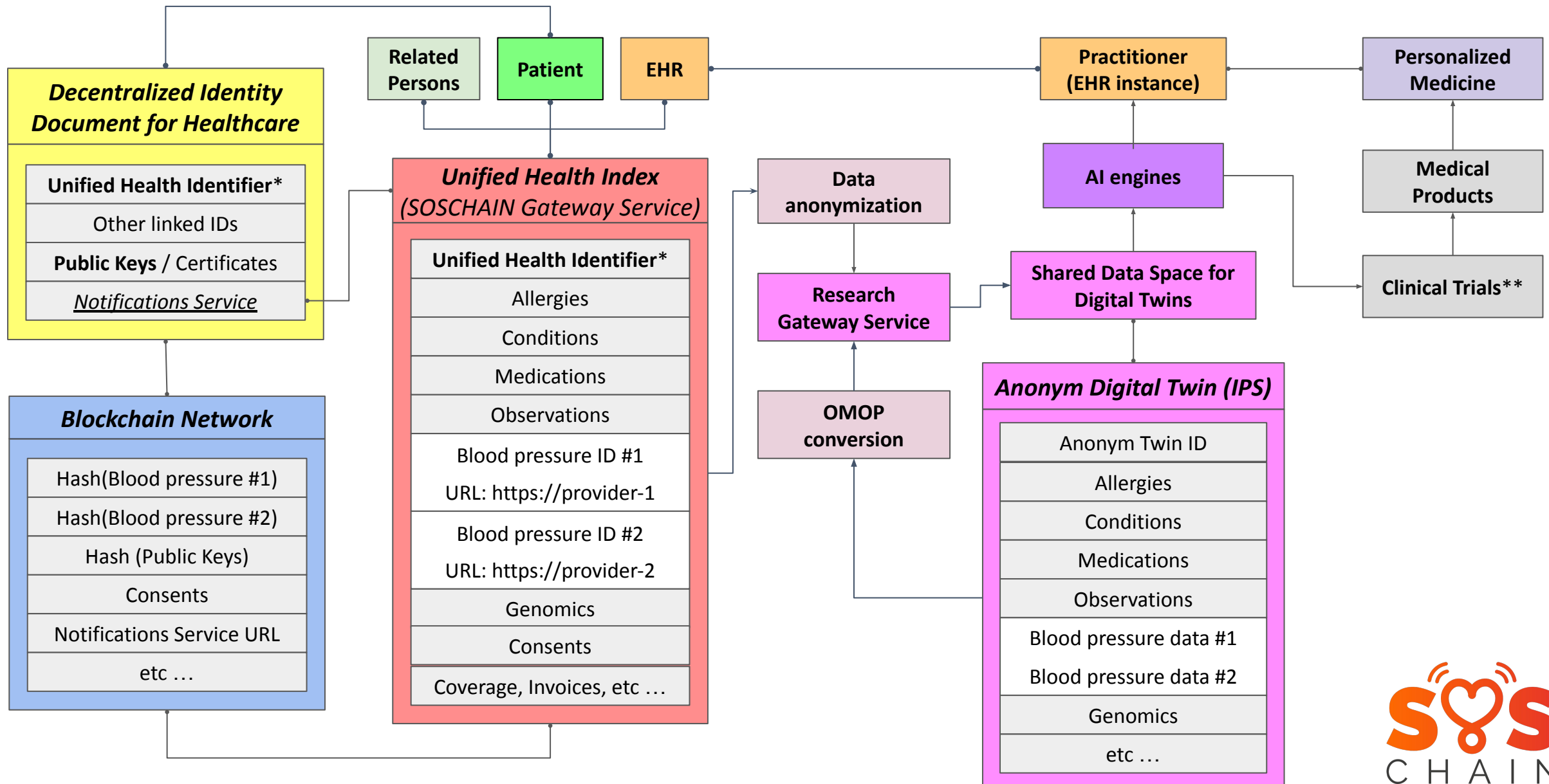
Resilient Architecture and Security by Design

Diagram for the Unified Health Index and Digital Twins

*Patent US 11,636,776; **Patent US 12,057,202

SOSCHAIN Shared Data Space with Unified Health Index

Medicinal Products

Pharmaceuticals

Hospital / Clinic

Clinical Trials**

EHR Software

Other EHRs

Private eHealth Networks

Public eHealth Networks

Wearables

Insurers (brokers)

Patient (consents, notifications, digital twins)

Data insights (AI)

SOSCHAIN Gateway Service

Patient's Unified Health Index*

Statistical Data (codes)

UHC Unified Health Chain

Notarization (documents)

Digital Twin (IPS anonymized)

Blockchain Network

Research Study Notarization

Shared Data Space for Care Continuity, Emergencies, Pandemics and Research Studies

SOS CHAIN

*Patent US 11,636,776; **Patent US 12,057,202*

Introduction to Cyber Attacks Types

SUMMARY

The Snake implant is considered the most sophisticated cyber espionage tool
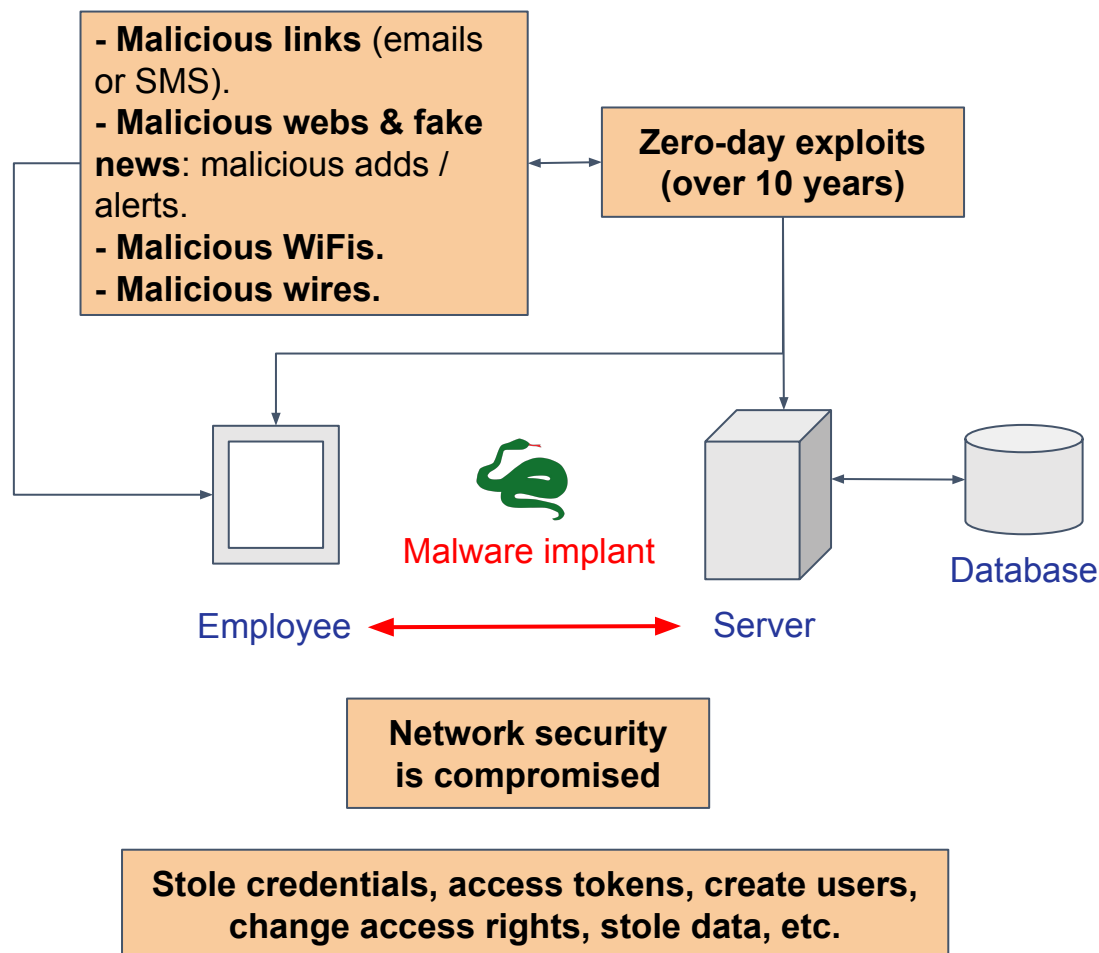
America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
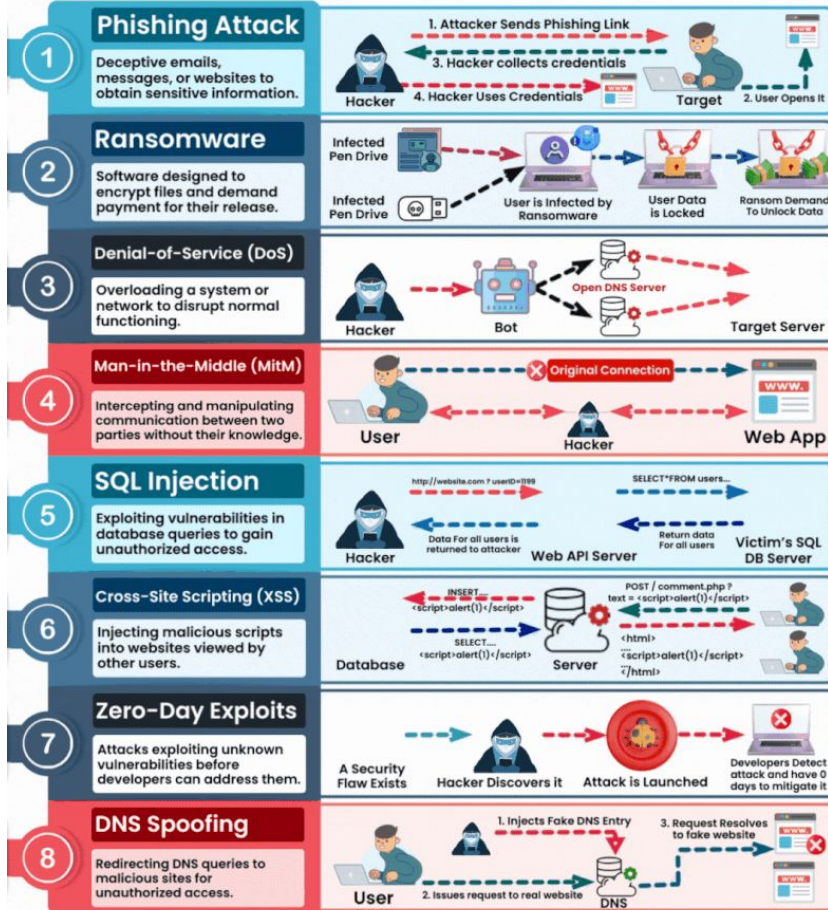
- **Malicious links** (emails or SMS).
- **Malicious webs & fake news**: malicious adds / alerts.
- **Malicious WiFis.**
- **Malicious wires.**

Zero-day exploits (over 10 years)

Malware implant

Database

Employee ←——→ Server

Network security is compromised

Stole credentials, access tokens, create users, change access rights, stole data, etc.

Brij Kishore Pandey · Save For Later

Top 8 Types of Cyber Attacks

1. Phishing Attack
Deceptive emails, messages, or websites to obtain sensitive information.
- 1. Attacker Sends Phishing Link
- 3. Hacker collects credentials
- 4. Hacker Uses Credentials
- 2. User Opens It
Hacker / Target

2. Ransomware
Software designed to encrypt files and demand payment for their release.
Infected Pen Drive — User is Infected by Ransomware — User Data is Locked — Ransom Demand To Unlock Data

3. Denial-of-Service (DoS)
Overloading a system or network to disrupt normal functioning.
Hacker — Bot — Open DNS Server — Target Server

4. Man-in-the-Middle (MitM)
Intercepting and manipulating communication between two parties without their knowledge.
User — Original Connection — Hacker — Web App

5. SQL Injection
Exploiting vulnerabilities in database queries to gain unauthorized access.
http://website.com ? userID=1199 — SELECT*FROM users...
Hacker — Data For all users is returned to attacker — Web API Server — Return data For all users — Victim's SQL DB Server

6. Cross-Site Scripting (XSS)
Injecting malicious scripts into websites viewed by other users.
Database — Server

7. Zero-Day Exploits
Attacks exploiting unknown vulnerabilities before developers can address them.
A Security Flaw Exists — Hacker Discovers it — Attack is Launched — Developers Detect attack and have 0 days to mitigate it

8. DNS Spoofing
Redirecting DNS queries to malicious sites for unauthorized access.
User — 1. Injects Fake DNS Entry — 2. Issues request to real website — DNS — 3. Request Resolves to fake website

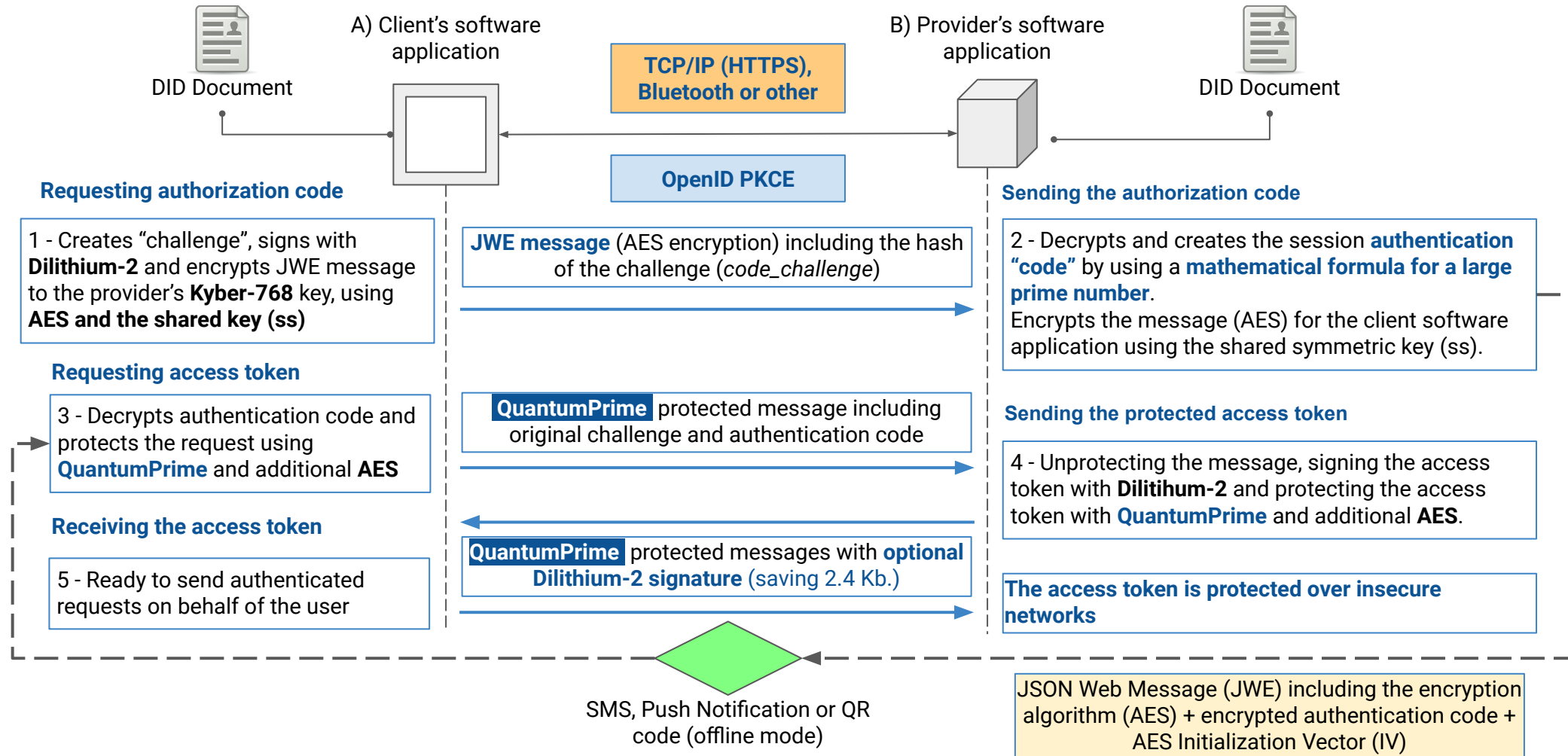# *QuantumPrime for Cybersecurity*

Prime numbers as "Lego" blocks to protect confidential information

A) `Formula:` *observable =* `base` `± E` , where `base` is a prime number, and `E` is a product of primes (Euclid's Theorem).

B) `Recursion:` applying the formula to each prime factor (up to a certain depth) allows for an **increase in complexity** (parts).

C) `Key:` which primes are used as `base`, in what `order of preference`, and the **level of** `recursion` applied.

1. `Easy integration:` sending mathematical expressions **as confirmation codes when performing operations** (email or SMS).

    1.1. *Example: the mathematical expression* **"2^2281-1"** *is encoded as* **"9RdfrxM5U9N"** *and generates a* **large prime** *(243 bytes).*

2. `Anonymization:` the formula produces a **unique hash of the information**, which is used as a public ID of the private data.

    2.1. *Security*: it is not possible to guess the key from a generated hash (prime numbers, order and recursion level).

    2.2. *Example*: Generation of **unique identifiers** (e.g., for each day or transaction), as an **extra layer of security** when protecting sensitive data, for example: **account number for payments**, **identification document**, **mobile phone number**, **device identifier** such as a **bluetooth device**, a **vehicle identification number** (VIN) for private vehicles, ambulances, military vehicles, etc.

    > Using as **preferred bases=[**`1021`, `23`**]** and **recursion=** `1` : `6543210 =` `1021` + `23` x 61 x 4663

       ID (SHA3-384): *0x4f03d5c44069aee9e16e83ec011c3f2d2d098ffe1735ad6ee6da0f8e40090d5a8a6db120bea86d391dfc16f74c60bfab*

    > Using as **preferred bases=[**`1021`, `23`**]** and **recursion=** `2` : `6543210 =` `1021` + `23` x (`23` + 2 x 19) x (`1021` + 2 x 3 x 607)

       ID (SHA3-384): *0xd49ebf3cb989bbec7b5180472d6a10c01f94caa6a5011c8367d8ab4732500ef6252d40f286f93988ca0b721351c10f75*

    > Using as **preferred bases=[**`1021`, `13`**]** and **recursion=** `2` : `6543210 =` `1021` + (`13` + 2 x 5) x (`13` + 2^4 x 3) x (`1021` + 2 x 3 x 607)

       ID (SHA3-384): *0xf12f876246224f1336325fe874ba68a504b9bc1b85431c2c76736d241a600d877f8038ed14825c82b057ea02b05bed7c*

Quantum-Resistant Security for the New Digital Era

**Secure login and data exchange for HTTP and Bluetooth protocols
by improved data protection mechanism** (based on the Financial API Security Profile)

QuantumPrime

DID Document

A) Client's software application

TCP/IP (HTTPS), Bluetooth or other

B) Provider's software application

DID Document

OpenID PKCE

Requesting authorization code

1 - Creates "challenge", signs with **Dilithium-2** and encrypts JWE message to the provider's **Kyber-768** key, using **AES and the shared key (ss)**

JWE message (AES encryption) including the hash of the challenge (*code_challenge*)

Sending the authorization code

2 - Decrypts and creates the session **authentication "code"** by using a **mathematical formula for a large prime number**.
Encrypts the message (AES) for the client software application using the shared symmetric key (ss).

Requesting access token

3 - Decrypts authentication code and protects the request using **QuantumPrime** and additional **AES**

QuantumPrime protected message including original challenge and authentication code

Sending the protected access token

4 - Unprotecting the message, signing the access token with **Dilitihum-2** and protecting the access token with **QuantumPrime** and additional **AES**.

Receiving the access token

5 - Ready to send authenticated requests on behalf of the user

QuantumPrime protected messages with **optional Dilithium-2 signature** (saving 2.4 Kb.)

The access token is protected over insecure networks

SMS, Push Notification or QR code (offline mode)

JSON Web Message (JWE) including the encryption algorithm (AES) + encrypted authentication code + AES Initialization Vector (IV)

SOS CHAIN

About Us

Fernando Latorre

CEO, CTO, co-founder
Cryptography specialist with experience in intellectual property protection and expertise in blockchain, healthtech, OpenID and decentralized identity technologies

Nuria Sala

COO, co-founder
Business and management experience, MBA, graduate in Nursing, and diploma in Health.

DevOps
Development and maintenance of software and computer systems, agile and high-quality software methodology.

Full-stack Developers
Specialists in both frontend and backend technologies for comprehensive application solutions across various sectors.

Graphic Designer
Specialist in creating visual narratives through innovative design and compelling aesthetics.

Business Model
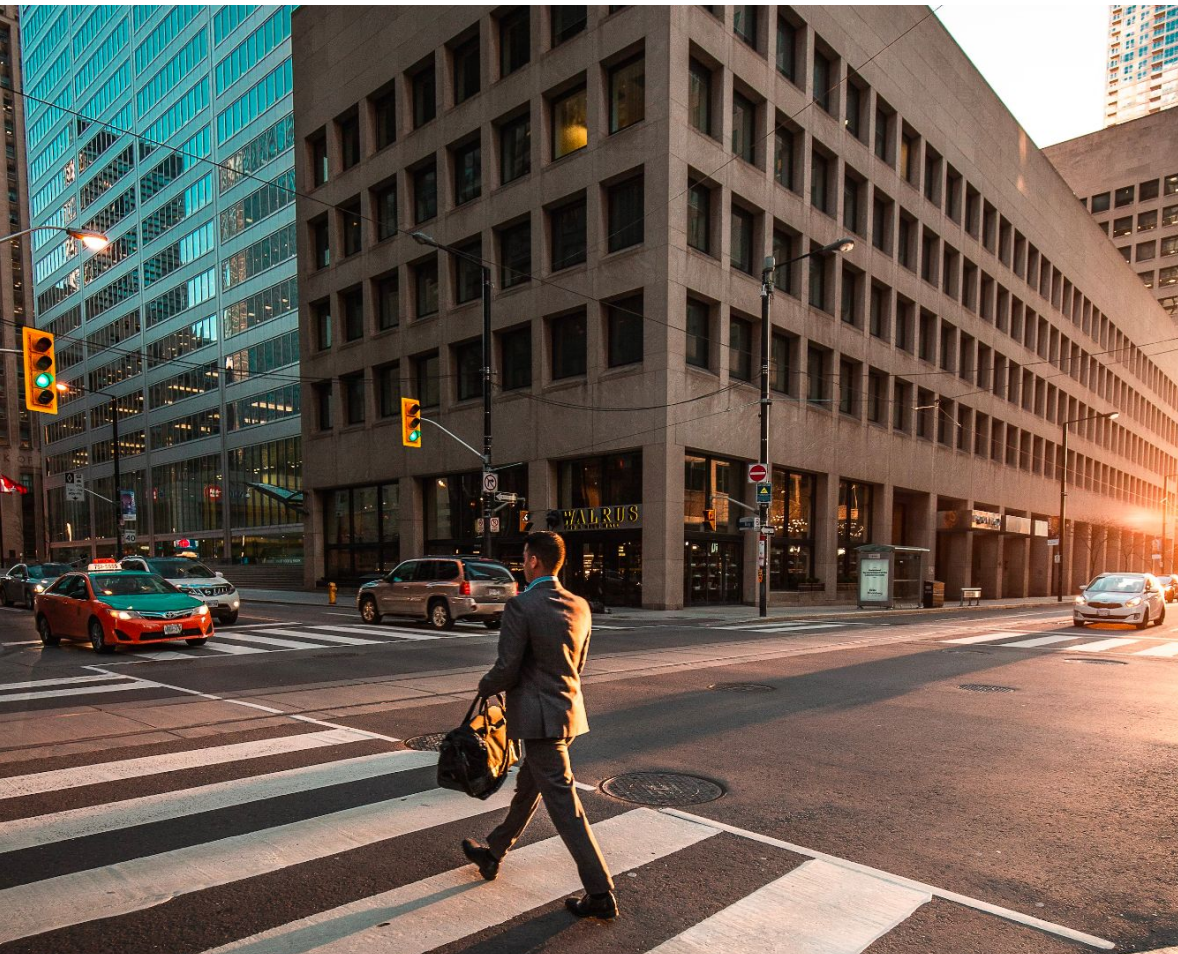
Third Party Integration via APIs
A gateway service enables integration with third-party systems, ensuring broad compatibility and flexibility.

Subscription model
Monthly or annual licensing for the gateway service, including regular updates and maintenance services to ensure high reliability and performance.

Subscription and licensing pricing
Costs varying with the number of licenses for data certifications and verifications.
- Micro-Business (up to 10 employees): $500 / month.
- Small Business (11 to 50 employees): $1,500 / month.
- Medium Business (51 to 250 employees): $5,000 / month.
- Large Business (more than 250 up to 1,000 employees): $7,500 / month.

Partners
Partnerships with software integrators and entities in the healthcare, insurance, clinical research sectors, offering possibilities for licensing agreements or volume pricing

Documentation: github.com/soschain/docs

Preview video: youtube.com/@soschain

Info: connecthealth.info/soschain