Using Strong Cryptography and Security

To Control Smart City Data

Isaac Potoczny-Jones
ijones@tozny.com
https://tozny.com

TOZNY

Tozny Background

Founded 2013 by Isaac Potoczny-Jones in Portland, OR

- Affiliated with Galois, the cybersecurity R&D company

Deep Experience with US Federal Government

- Current projects: NIST Trusted Identities Group; DARPA, and Galois

Won and executed cybersecurity for 14 years

- Team won and executed contracts for over a decade: DARPA, DHS

TOZNY

Deep questions for Smart Cities

- **Ownership**: Who owns the data?
  - A legal question that can be answered with policy
- **Storage**: Who houses the data and where?
  - A practical question about the legal rules for access and security
- **Access**: Who can access the data?
  - A combination of security, access control, and legal policy
- **Subject**: Who is the data about?
  - More often than not, they don't own it, store it, or even access it.

But the most important question:

Who *Controls* the Data?

Control is the overlap of ownership, storage, access, and subject

- Lots of modern business runs on the premise that you are the product, not the customer.
- In other words, give up your data privacy for free services
- This should not be the model for smart cities.

How can we put the right people in control?

TOZNY

TozStore Uses Cryptography to Control Data

Product and protocol construction

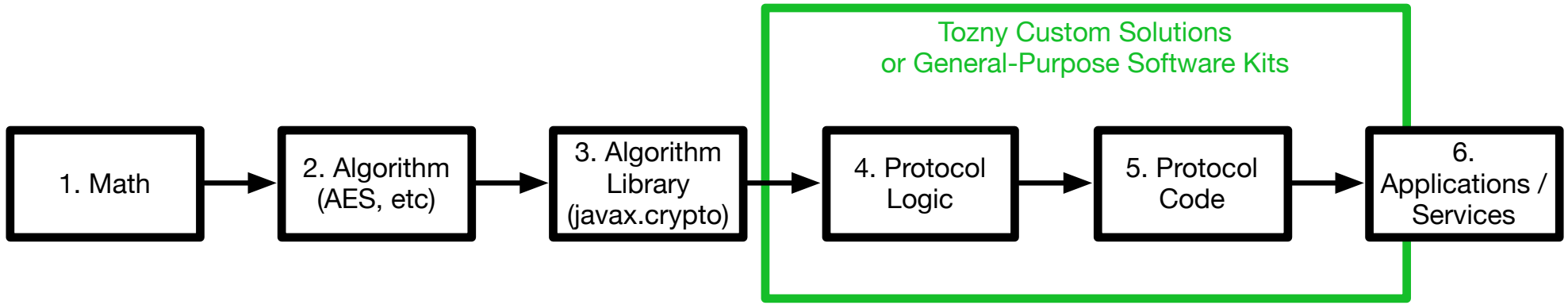
- We layer our approaches on verified cryptography

User and Programmer Experience

- The biggest challenge to good crypto is that it's hard to use

Work across crypto suites and problem spaces

- Successfully applied NIST suites, libsodium, at rest, in transit, etc.



TOZNY

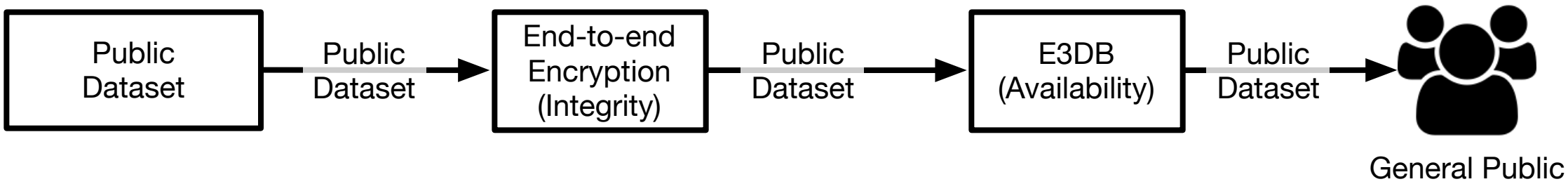
A different approach to cryptography

Not just about security

- Leverages key management to say who controls this data
- No matter where it's stored, who owns it, or who it's about
- Examples:
  - Maintain control of data shared with 3rd party contractors
  - Give data subjects actual control over who accesses data about them
  - Remove control from the data storage system
  - Secure data no matter what system it gets backed up to

TOZNY

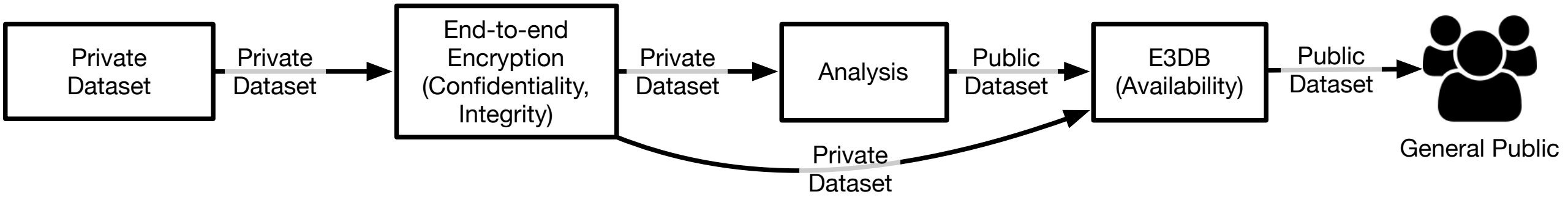
Public Datasets: Control who can change



- Provide integrity and availability
- Easy to access, general purpose API
- But smart city datasets are about more than just public data

TOZNY

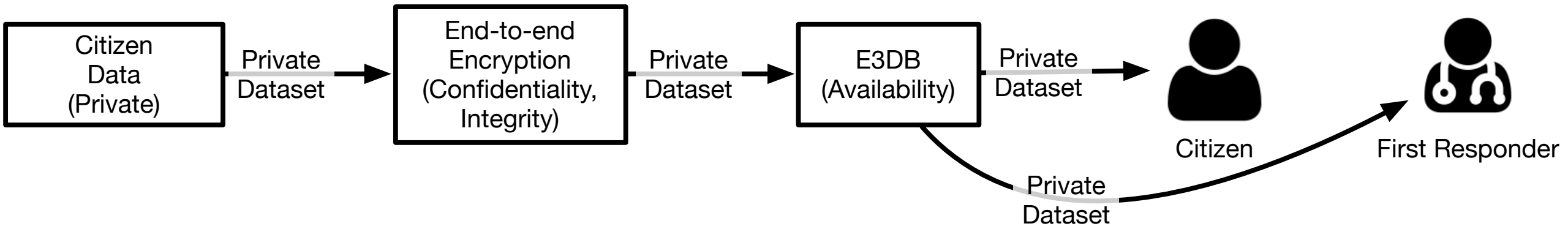
Extracting public data from private data



- Provide security for private data
- Allow privacy-preserving transformations
- Provide integrity and availability to public data

TOZNY

Private Datasets: Control who can access



- Provide confidentiality for private data
- Put citizens in control

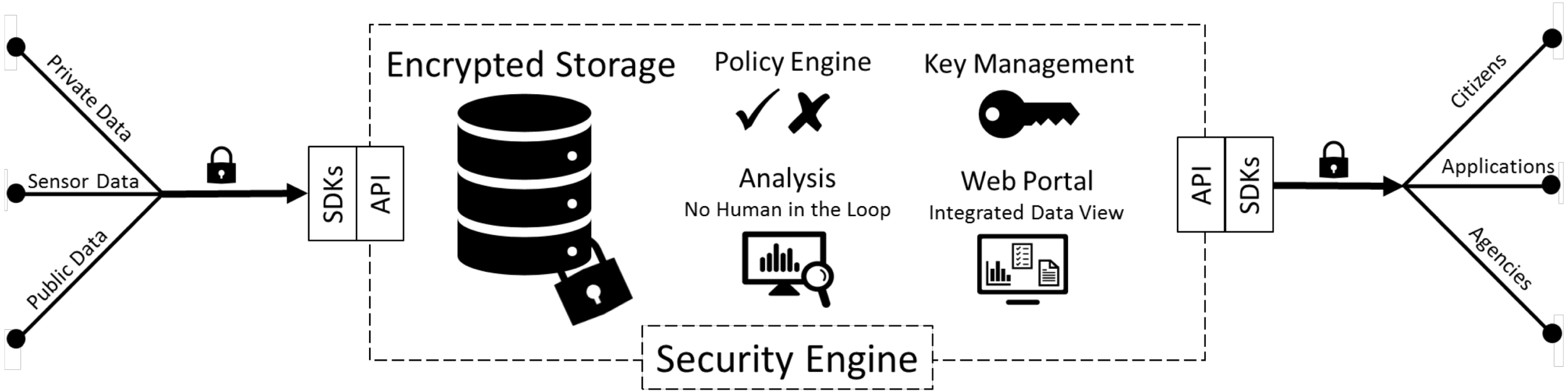
TOZNY

TozStore

- High-end, innovative crypto
  - We keep up on the latest approaches and vulnerabilities so you don't have to
  - We did it right and vetted it extensively
- Insanely easy to integrate InnoVault
  - SDKs: Ruby, PHP, Go, Java, HTML/CSS, JavaScript, iOS, Android
  - October: Node, Python, … What's your favorite?
- Easy key management, policy control, and queries
  - YOU get to say who gets access to data
  - Which servers, clients, employees, users, …
- Delivered as SAAS or SDK with strong backups and archiving
  - Use our servers in our environment or yours
  - Use our SDKs to store data in your own databases

TOZNY

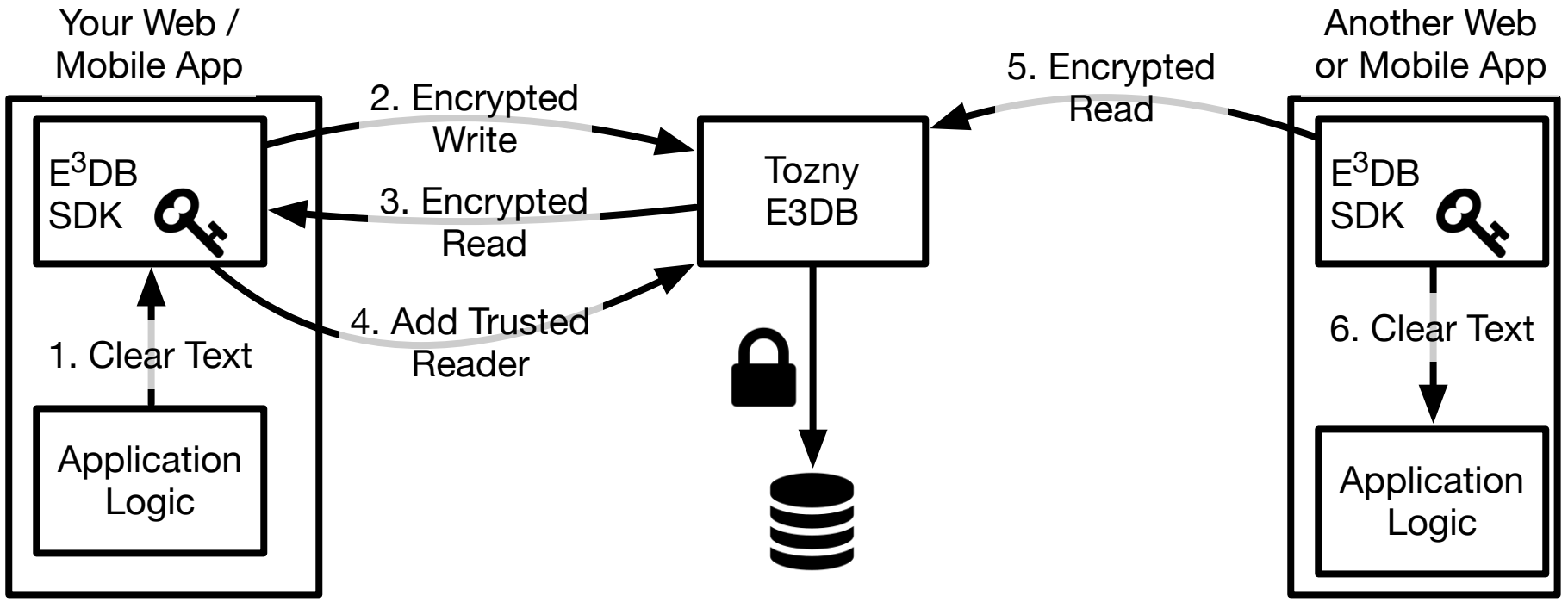
Secure City Software Kit



- Support cryptography directly between users
- 3rd parties don't touch the unencrypted data
- And neither does E3DB

TOZNY

Approach: Client and server SDKs



- Any developer can bake this into their application
- Available for a wide variety of languages & platforms

TOZNY

Primitives: Operate on JSON Data

- Key Gen: Generate ECC (asymmetric) keys, register, optional backup
- Encrypt / Decrypt: Data is JSON and natural to the language
- Write: Encrypt data and send to E3DB with optional query metadata
- Read: Fetch data, decrypt, check signatures
- Query: Search metadata
- Share / Authorize: Efficient cryptographic control plus access control

TOZNY

Identity Management

- Trusted login – you are who you say you are
- User Attributes – what can various parties find out about you
- Single sign-on across city services – convenience & consistency
- Would love to help deploy a user-centric city identity infrastructure
- Could be based on open source IdM like KeyCloak or Gluu

TOZNY

Status

- The product is built and deployed at scale
- Already funded by DHS privacy group to work with Portland and other cities on privacy-preserving approaches to smart city data collection
- We have room for a pilot on this contract to secure your data set
- Looking for partners: platform, problems, projects, and funding

TOZNY

Questions

- Do you agree that this platform addresses key challenges?
- What barriers to adoption / integration do you see?
- How should this be offered to increase impact and sustainment?

TOZNY

Discussion

Questions

TOZNY

Thank You!

Isaac Potoczny-Jones
ijones@tozny.com
https://tozny.com

TOZNY