Using Personal Portfolios to Manage Customer Data

Aimilia Tasidou, PhD student
Algorithms and Privacy Research Unit
Department of Electrical and Computer Engineering
Democritus University of Thrace, Greece

Joint work with assistant professor P.S. Efraimidis

Aims and results

- Goals:
  - Transaction information **at the owner's control**.
  - **Customer data management** easier for companies.
  - Privacy-preserving **utilization** of transaction data.
- Results:
  - Designed a **Portfolio system** where individuals' transaction data are stored and managed by its owner.
  - **Privacy preserving, legitimate** way to access **accountable** transaction information.

Presentation outline

- Motivation
- Portfolio approach
  - Concepts and architecture
  - Building blocks
  - Functionality
  - Applications
- Conclusions
- Future work

Motivation

Transaction data handling today

- **Customer profiles** record transaction and personal information.
- **No option** to perform transactions anonymously.
- **Loyalty cards** offer privileges in exchange for **data recording**.
- Collected data can **compose an individual's detailed profile** revealing sensitive information about them.

$\Rightarrow$ Shopping profiles can be a significant source of private information leakages.

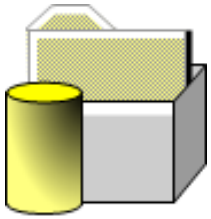
Economic aspects of privacy

- Companies **profit** out of using individuals' transaction information.
- Customer information processing is a **viable task** and brings important benefits to the marketplace.
- The **goal of privacy** protection is **not to lock** transaction information away from any possible use.
- A **privacy-preserving** and **accountable** way to access and **utilize** individuals' transaction information is needed.

The Portfolio Approach

Concepts and architecture

The concept



- Portfolio:
  - **Owned** by an individual.
  - Stored **locally** at their side.
  - Contains individual's **transaction history**.
  - Controlled access, under **owner's consent.**
- Desired attributes:
  - **Protect** transaction profile.
  - **Enable utilization** of transaction data.
  - **Ensure accountability** of revealed information.

Portfolio entities

- The individual.

Portfolio entities

- The individual.
- Shops and service providers .

Portfolio entities

- The individual.
- Shops and service providers .
- Companies (data consumers).

Portfolio entities

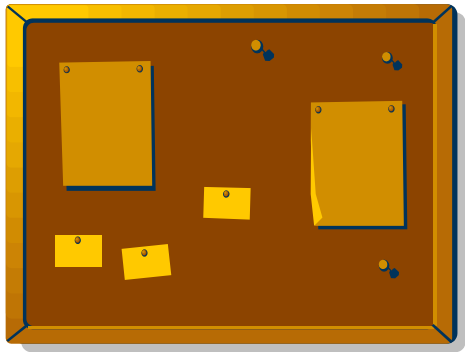
- The individual.
- Shops and service providers .
- Companies (data consumers).
- An identity provider.

Portfolio entities

- The individual.
- Shops and service providers .
- Companies (data consumers).
- An identity provider.
- A notarization service.

Portfolio entities

- The individual.
- Shops and service providers .
- Companies (data consumers).
- An identity provider.
- A notarization service.
- A notice board.



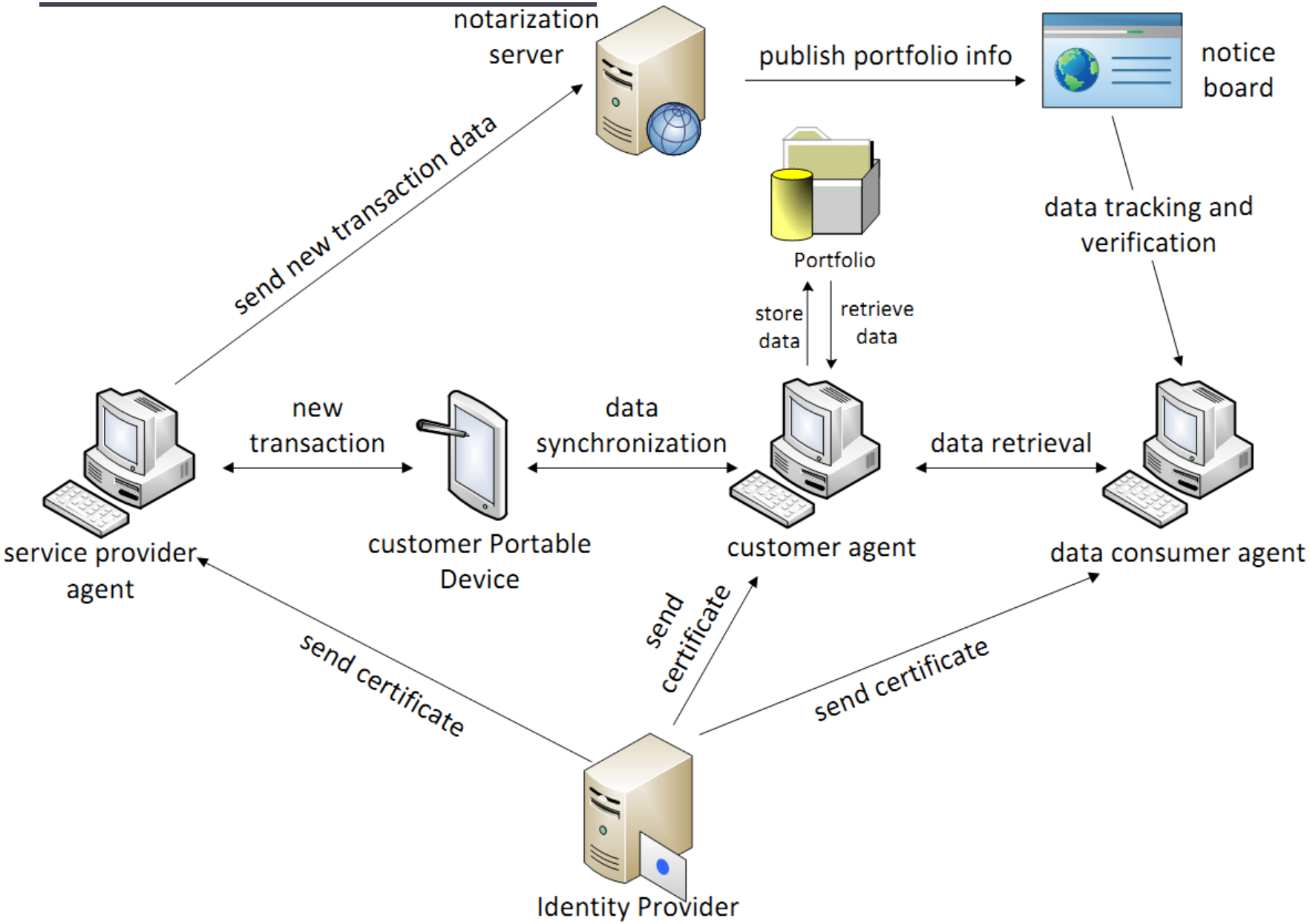
Portfolio entities

- The individual.
- Shops and service providers .
- Companies (data consumers).
- An identity provider.
- A notarization service.
- A notice board.

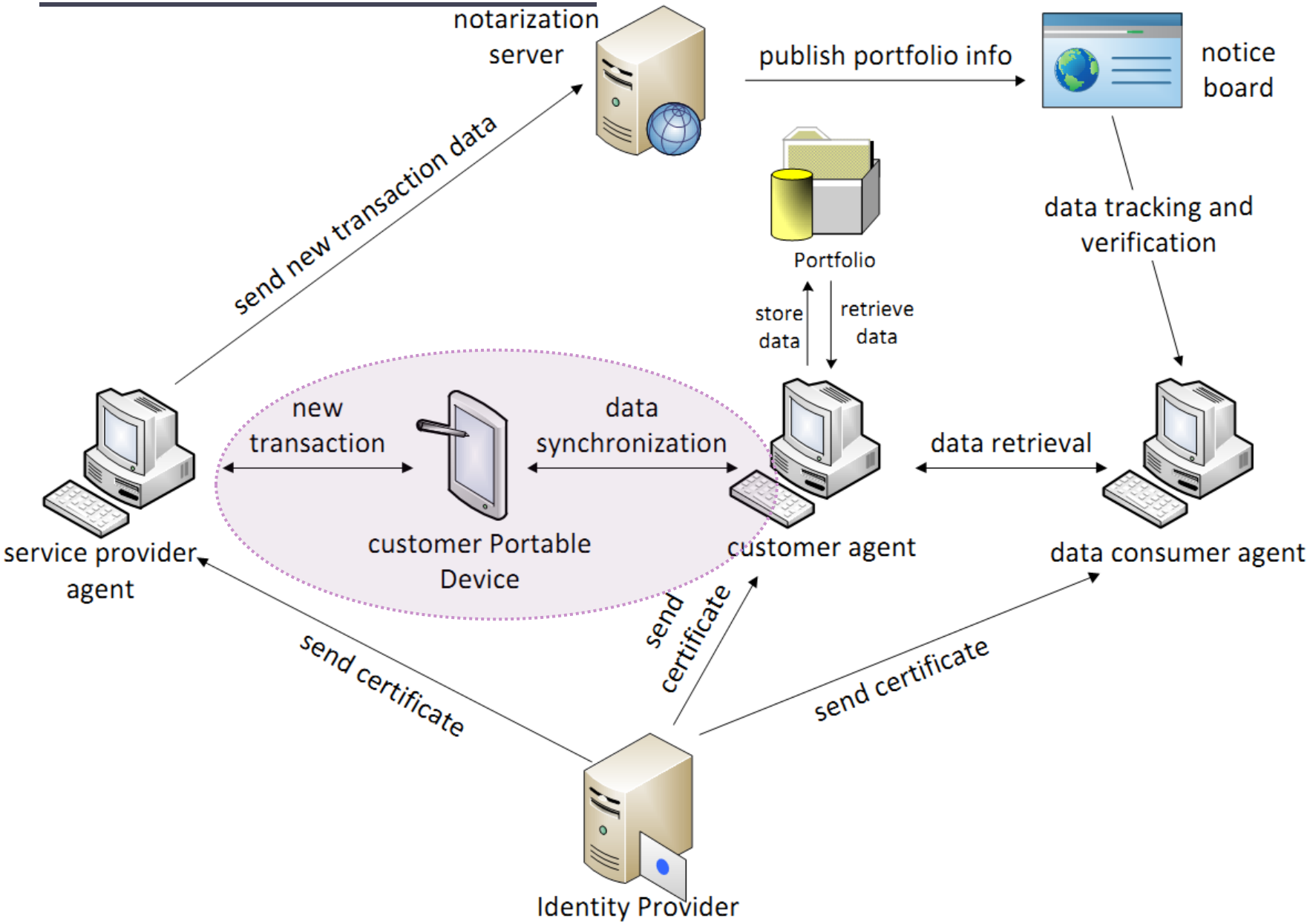
- Individuals, shops and companies are all Portfolio users.

- The main system components are the following:
  - The Portfolio that belongs to an individual.
  - The software agent (A_u) of user U.

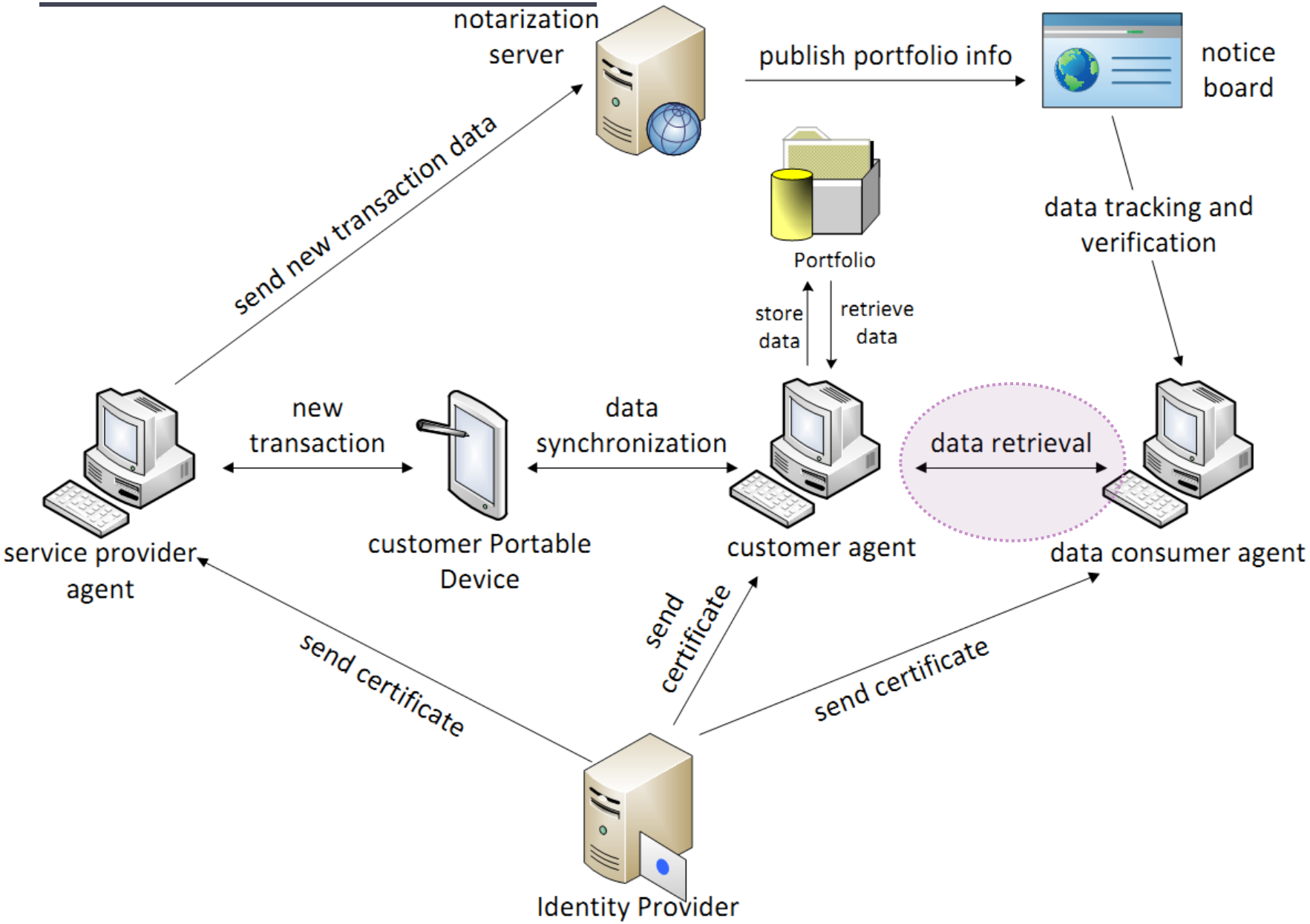
Portfolio architecture



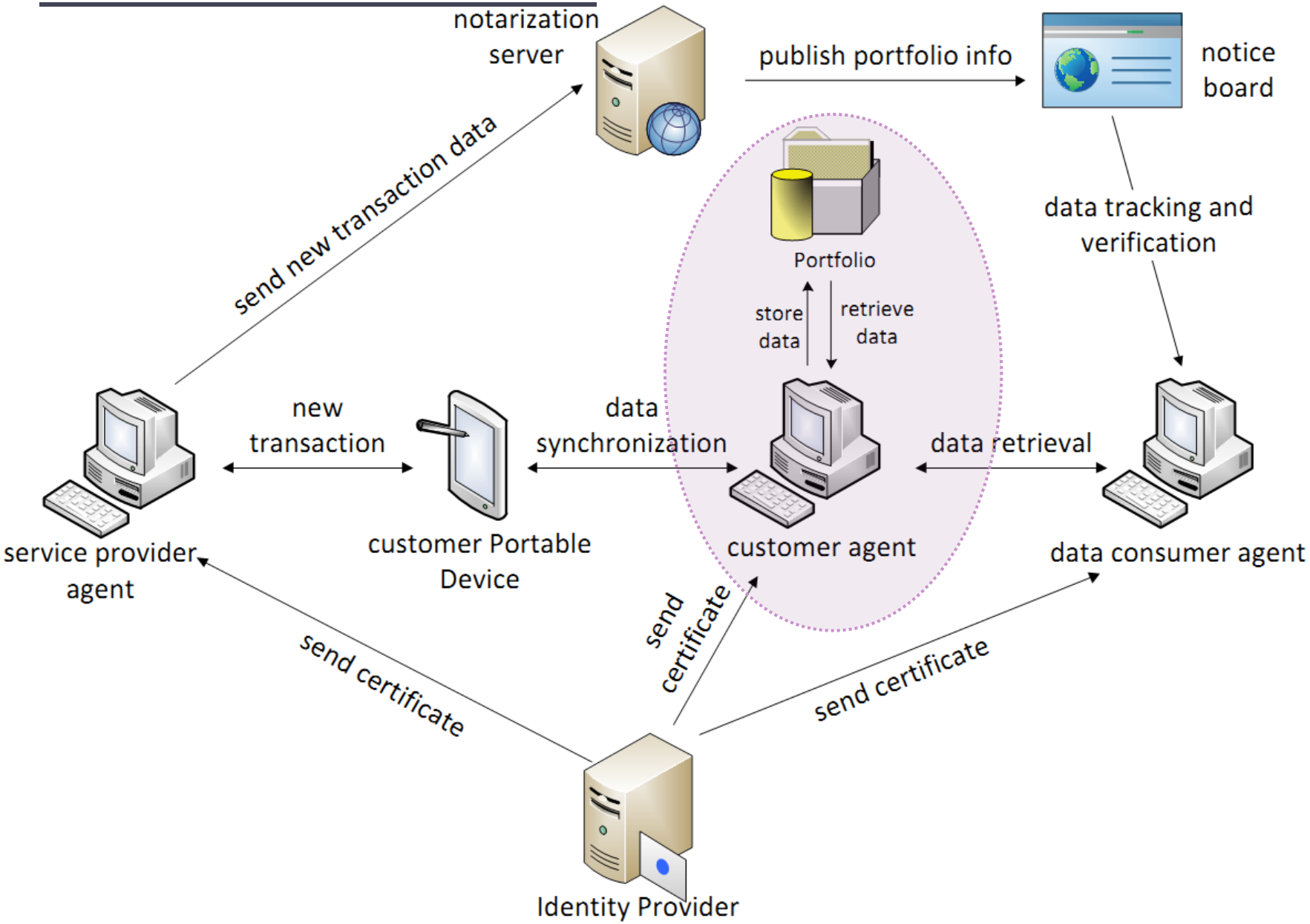
Portfolio architecture



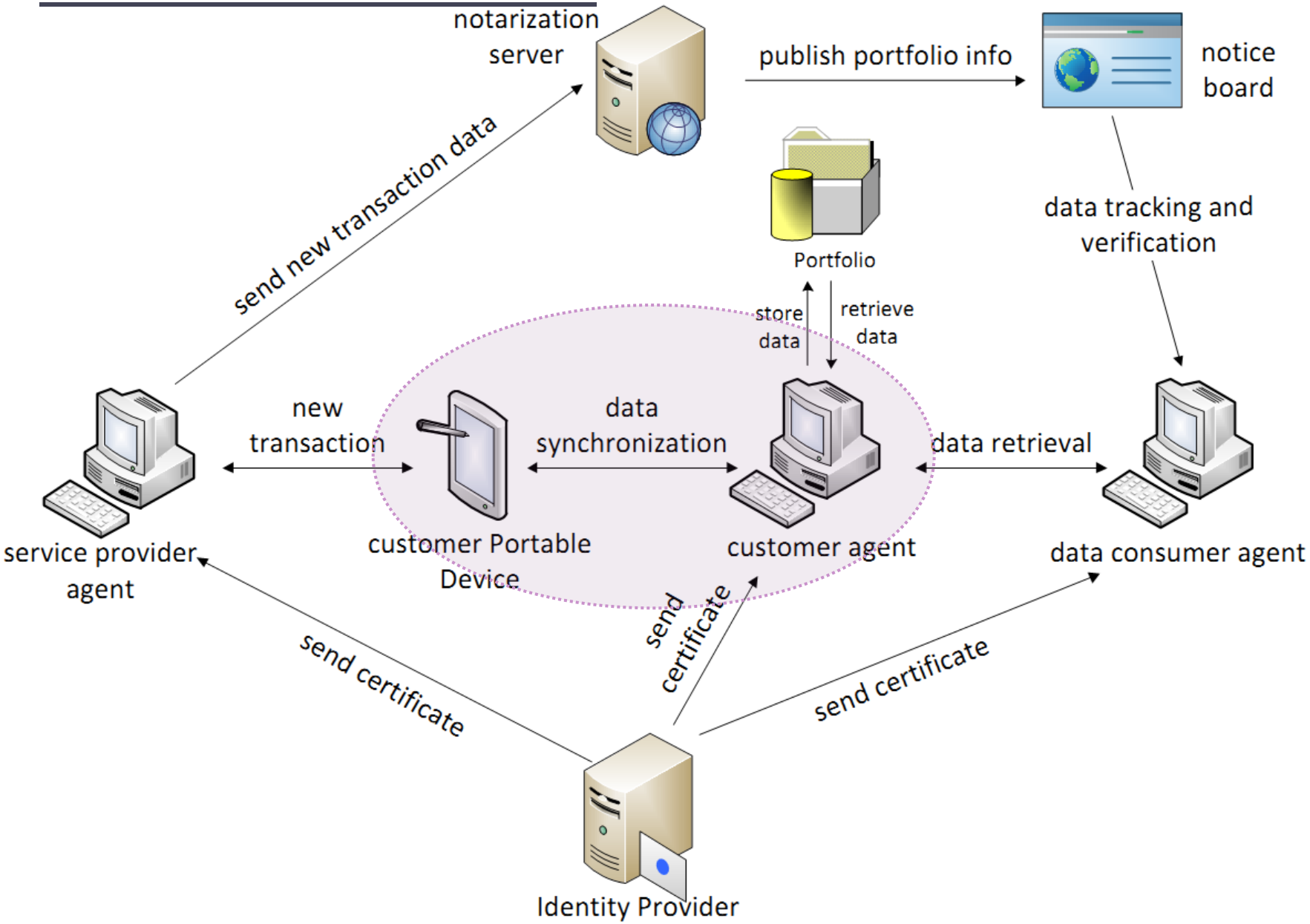
Portfolio architecture



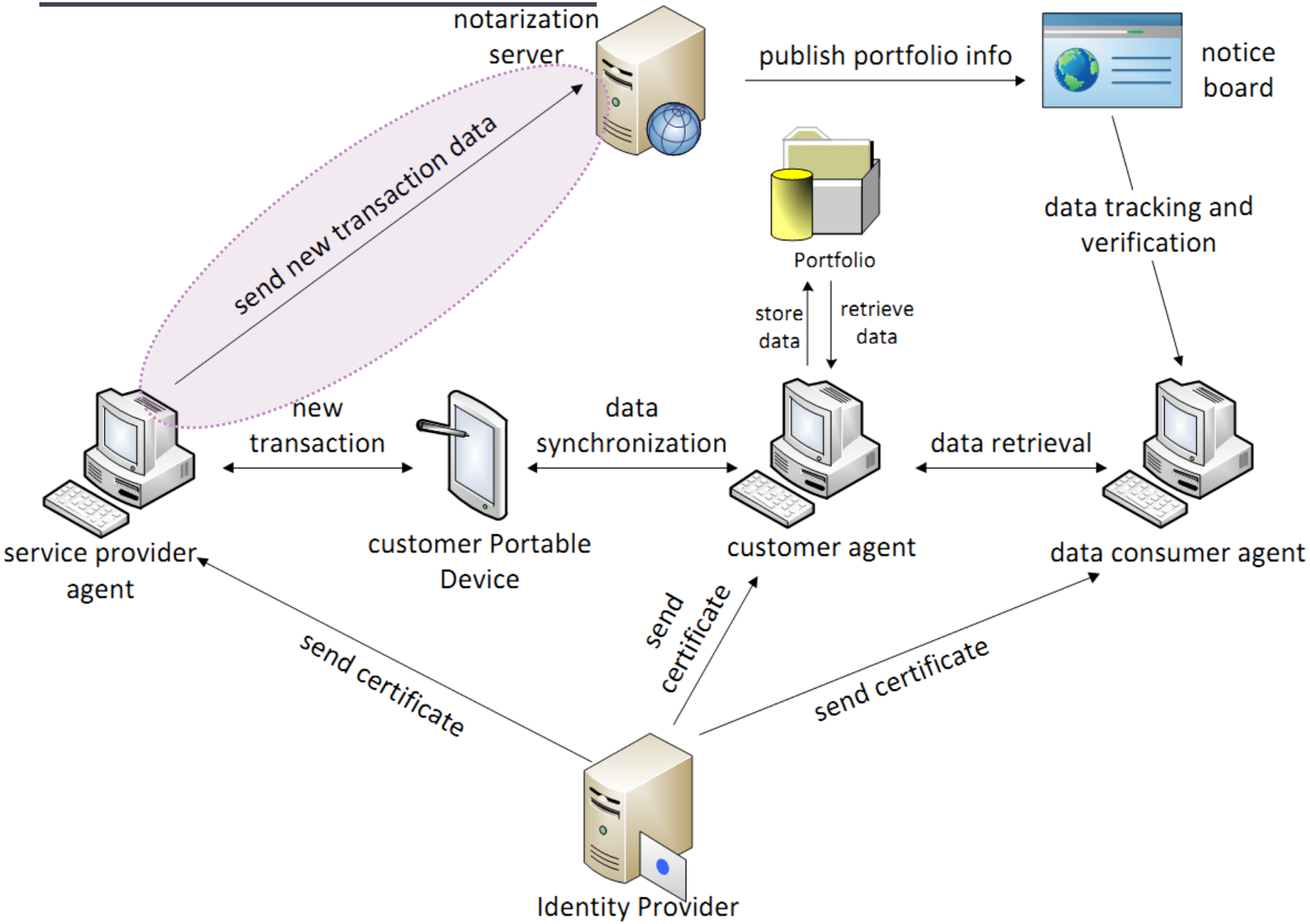
Portfolio architecture



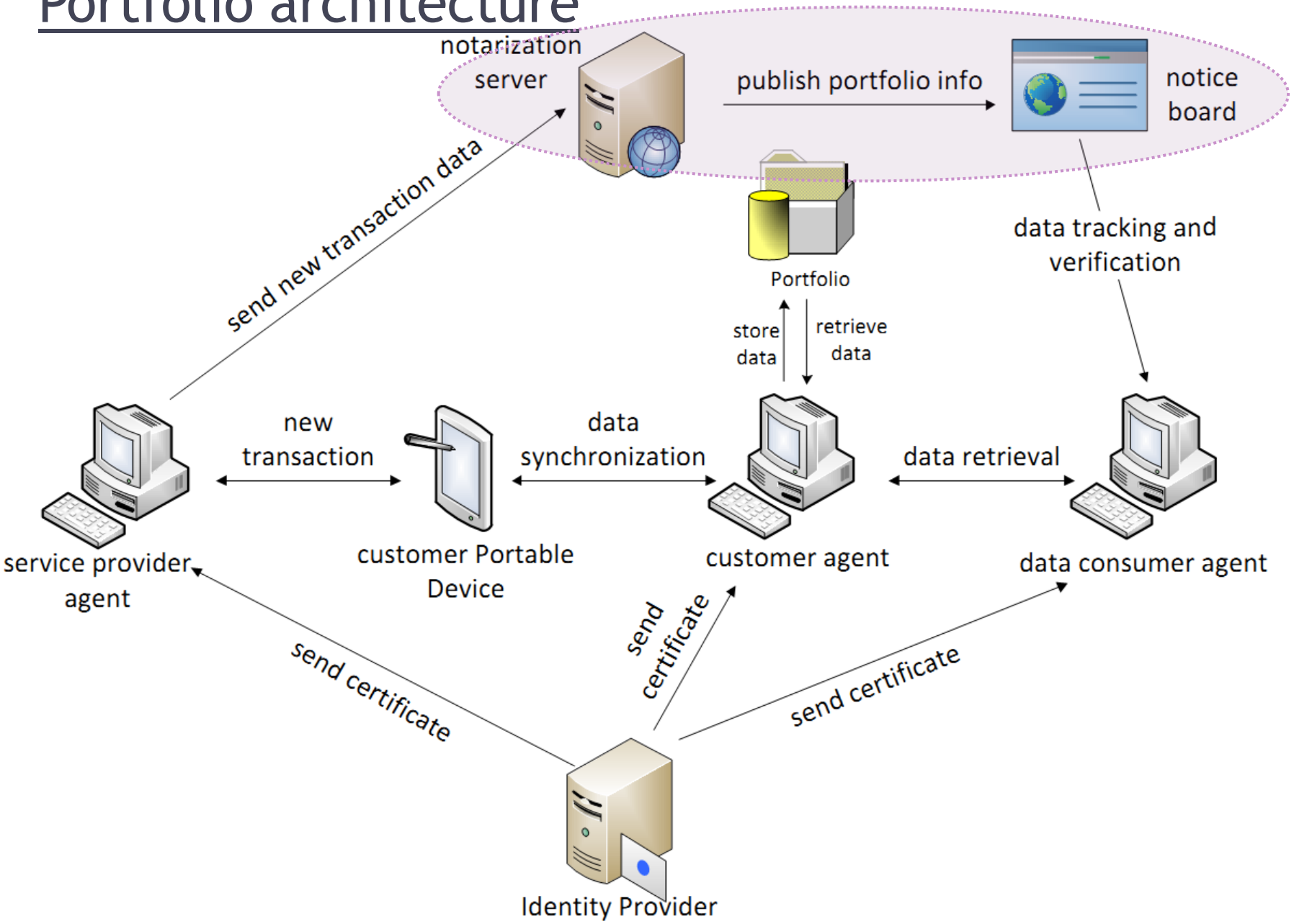
Portfolio architecture



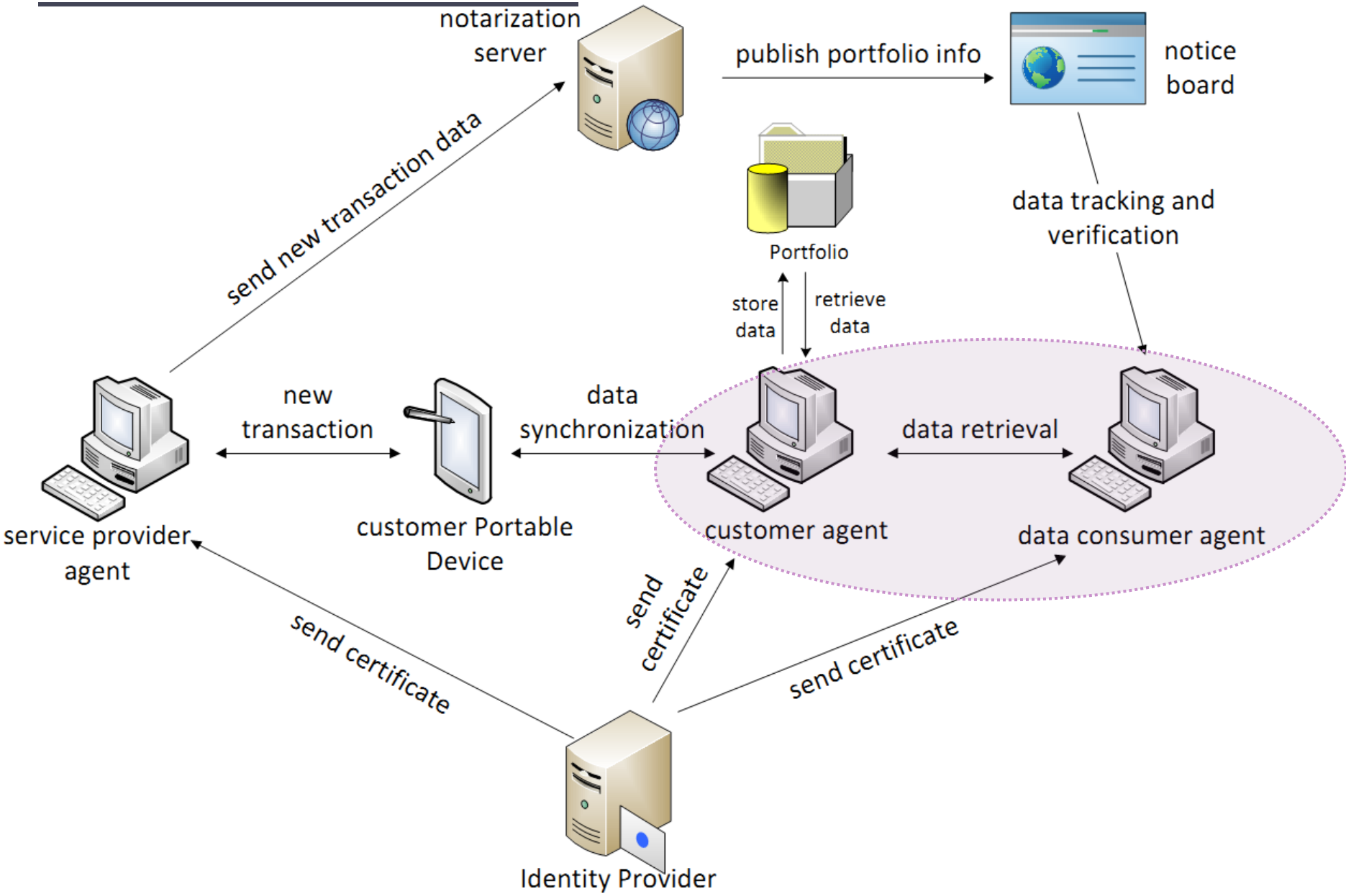
Portfolio architecture



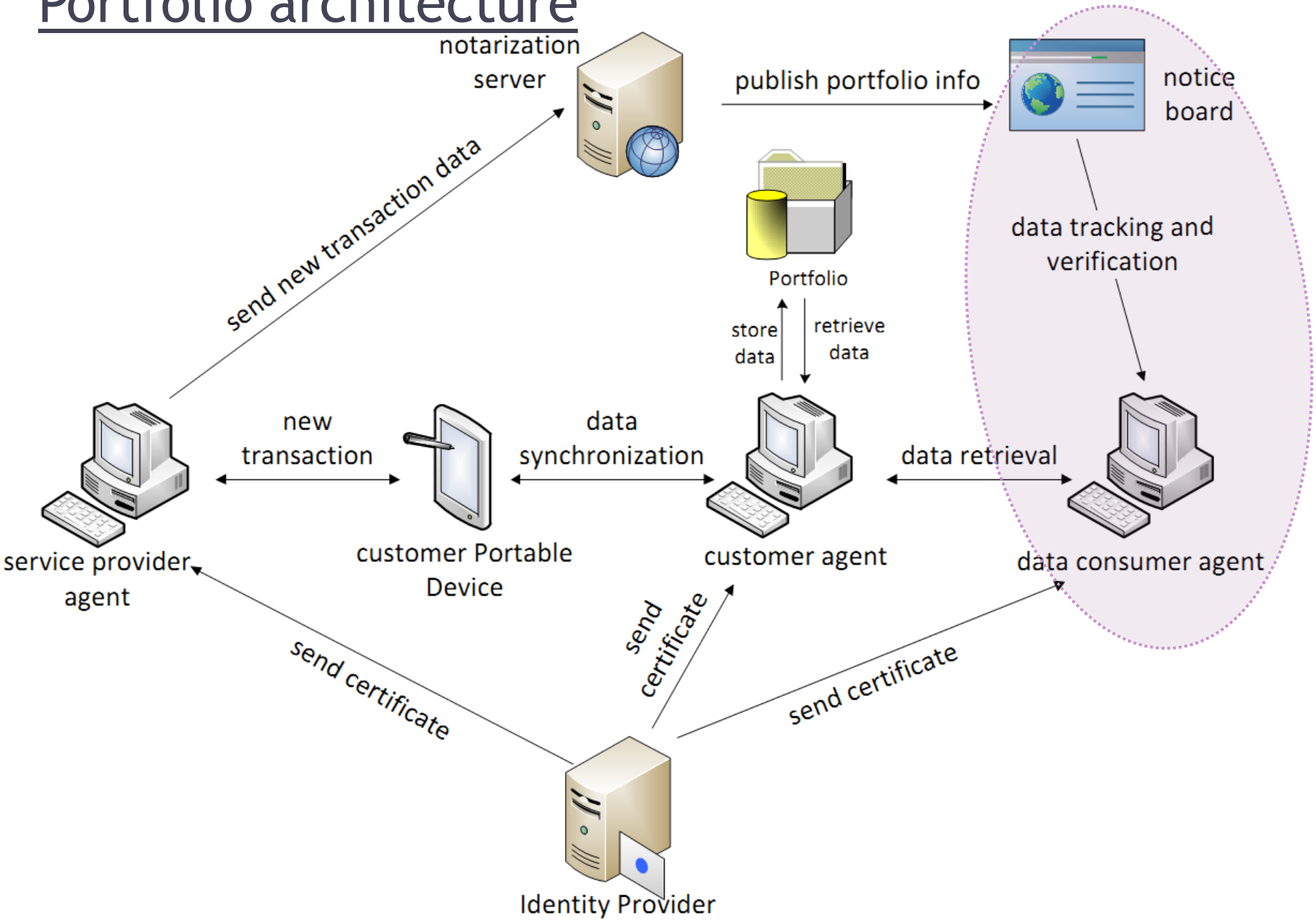
Portfolio architecture



Portfolio architecture



Portfolio architecture



The Portfolio Approach

Building blocks

Anonymous Credentials

- A private credential system like the one described by Camenisch et. al. (Eurocrypt 2001) offers:
  - Different **unlinkable** pseudonyms based on the same credential.
  - **Unforgeability** of credentials.
  - **Unlinkability** of credential showings.
  - Anonymity **revocation**.

Public Key Encryption with Keyword Search

- PEKS (Boneh et. al., Eurocrypt 2004) allows for **keyword searches within encrypted data**.
- **Transactions encrypted** with the owner's public key .
- **Retrieval** achieved using **search trapdoors** that match the **PEKS keywords** of the transactions.
- PEKS keywords posted on the **notice board** to track and verify transaction data.

Tamper Detection

- Tamper detection mechanisms (Snodgrass et. Al., VLDB 2004) are used **to ensure data accountability**.
- Individuals should not be able to **alter**, **remove** or **hide** transactions from their portfolio, thus presenting invalid profile attributes.
- The **notarization service** is introduced in the portfolio architecture to serve towards this end.
- **Digital signatures** are used to **prohibit tampering** with transaction contents.

The Portfolio approach

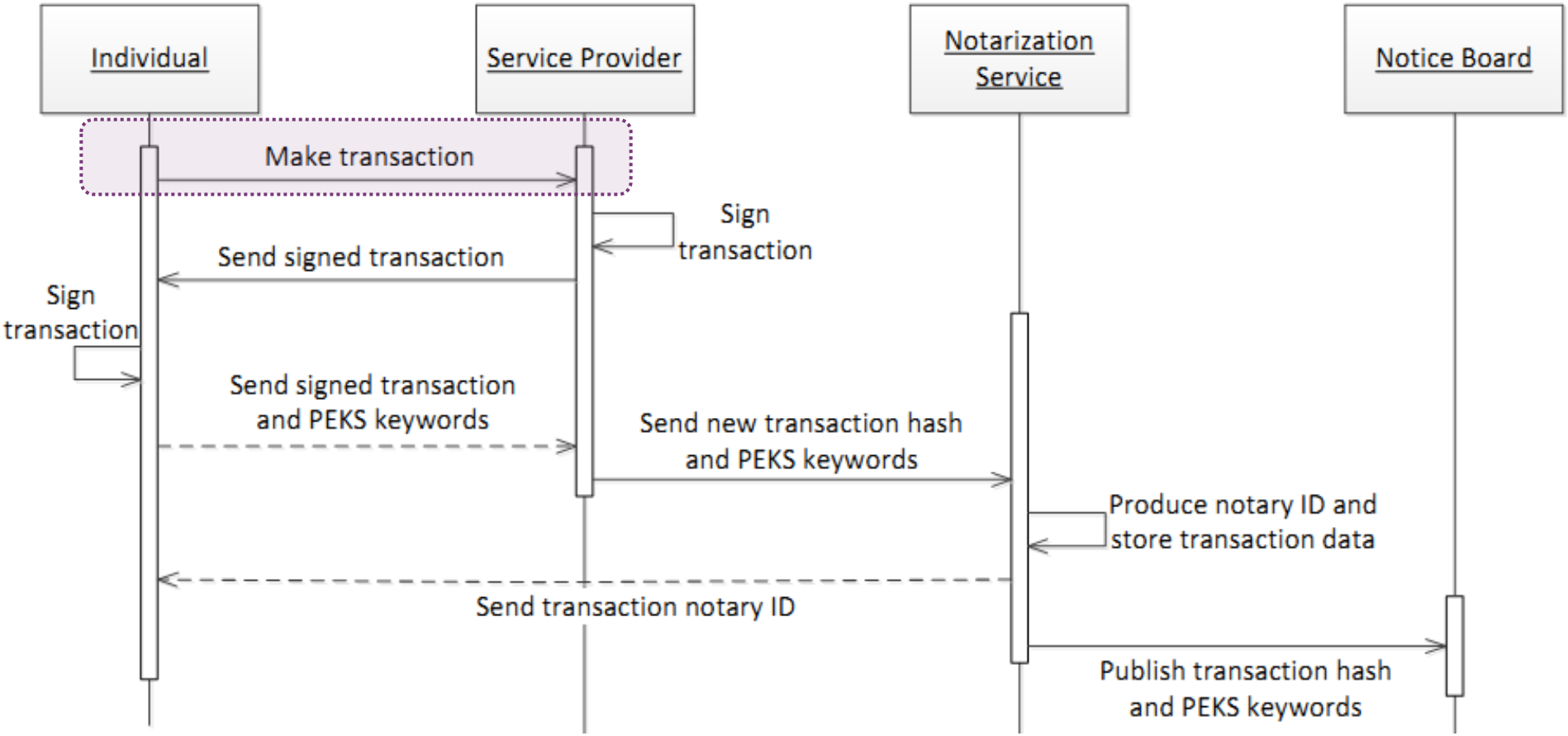
Functionality

Portfolio functionality

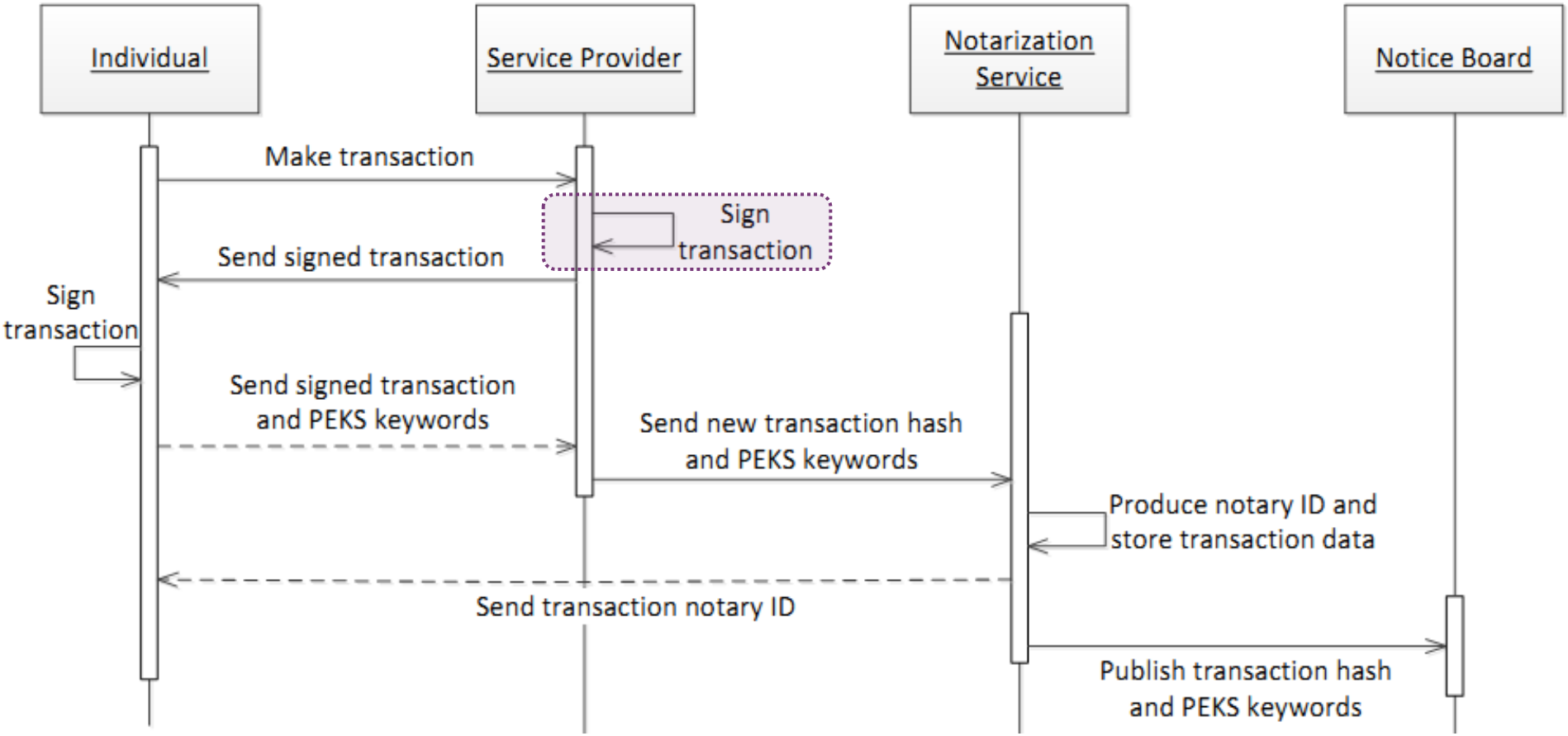
- Two protocols were designed to complement agent interaction in the portfolio system and demonstrate its functionality:
  - Transaction insertion protocol.
  - Data retrieval protocol.

- Both protocols achieve the desired functionality, while offering privacy protection and information accountability.

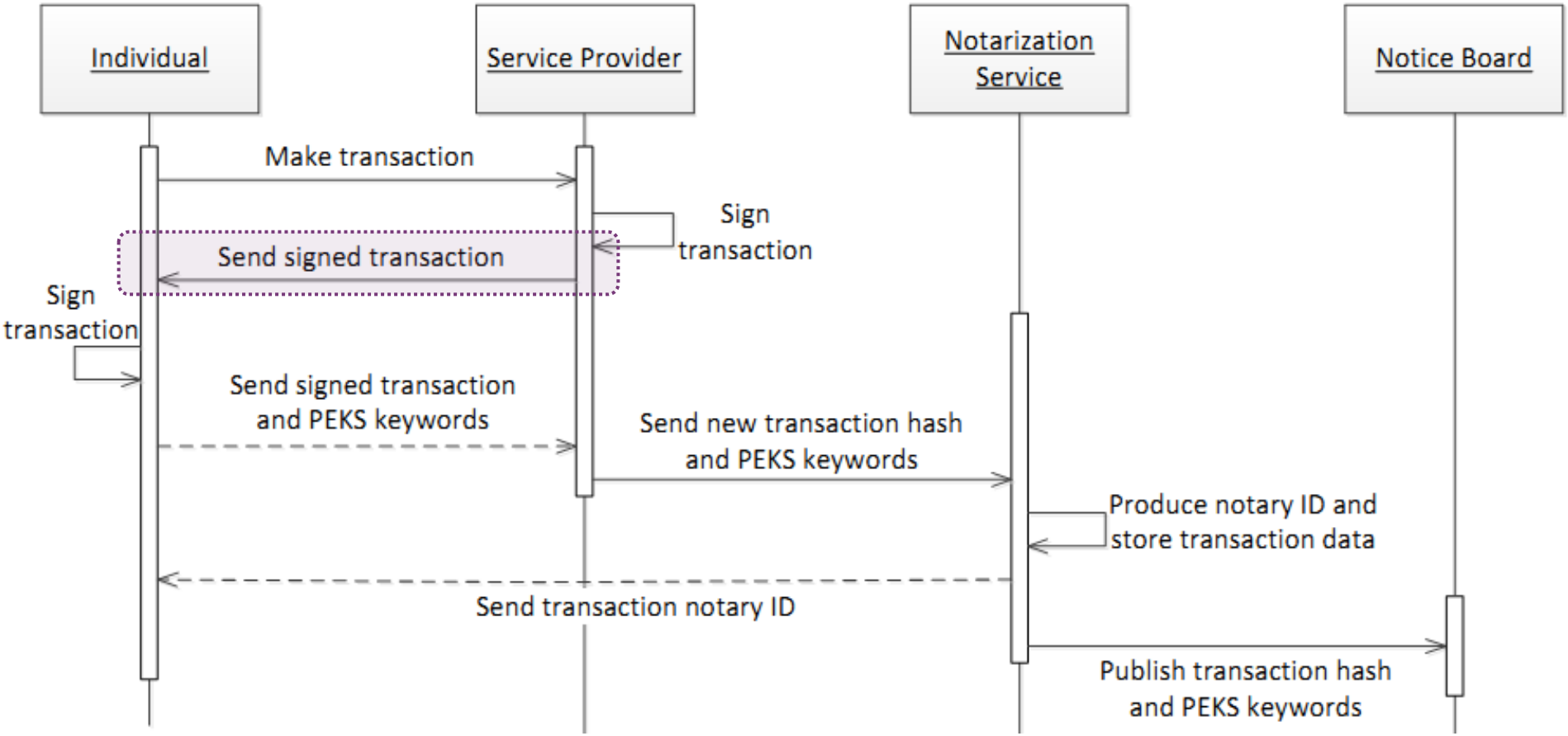
Transaction Insertion Protocol



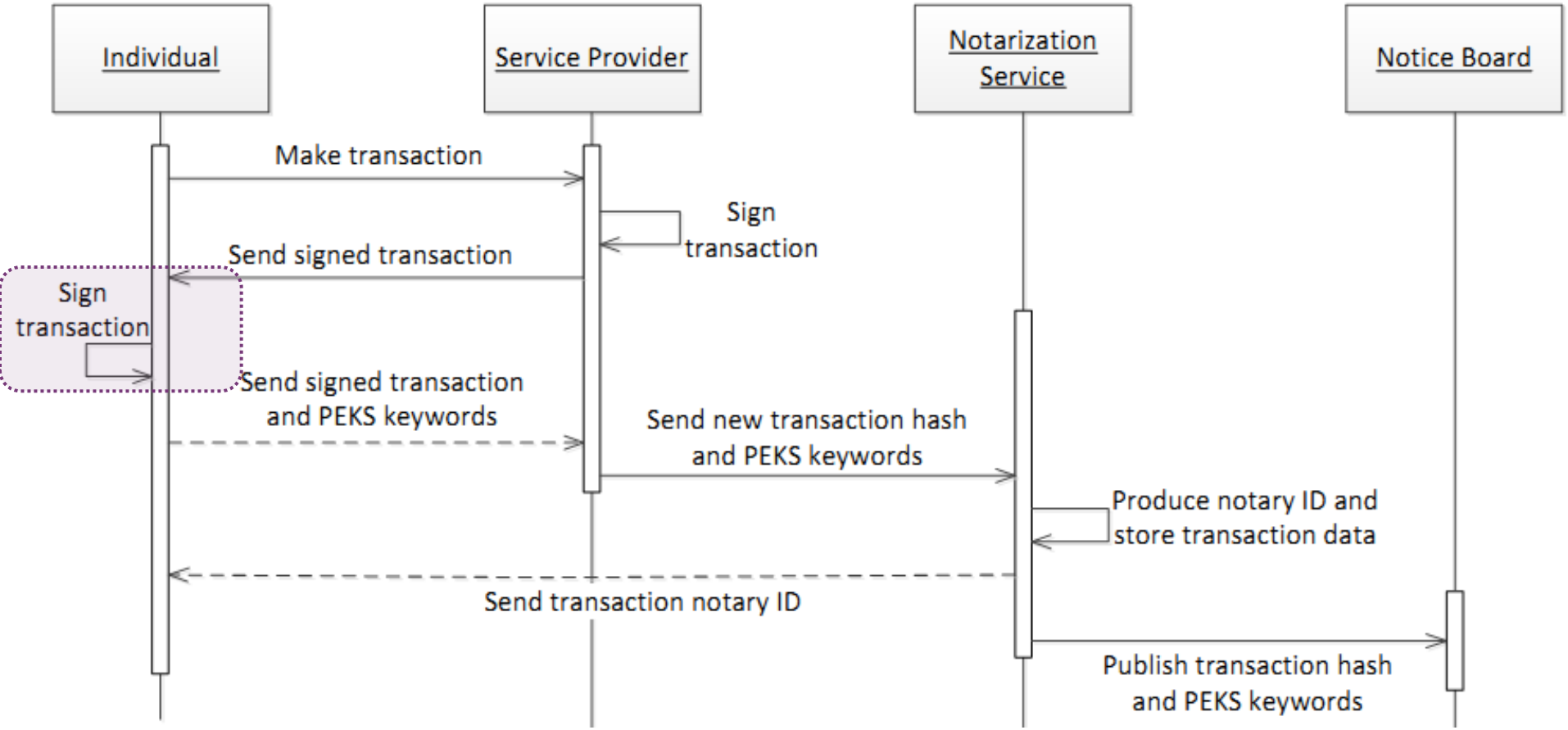
Transaction Insertion Protocol



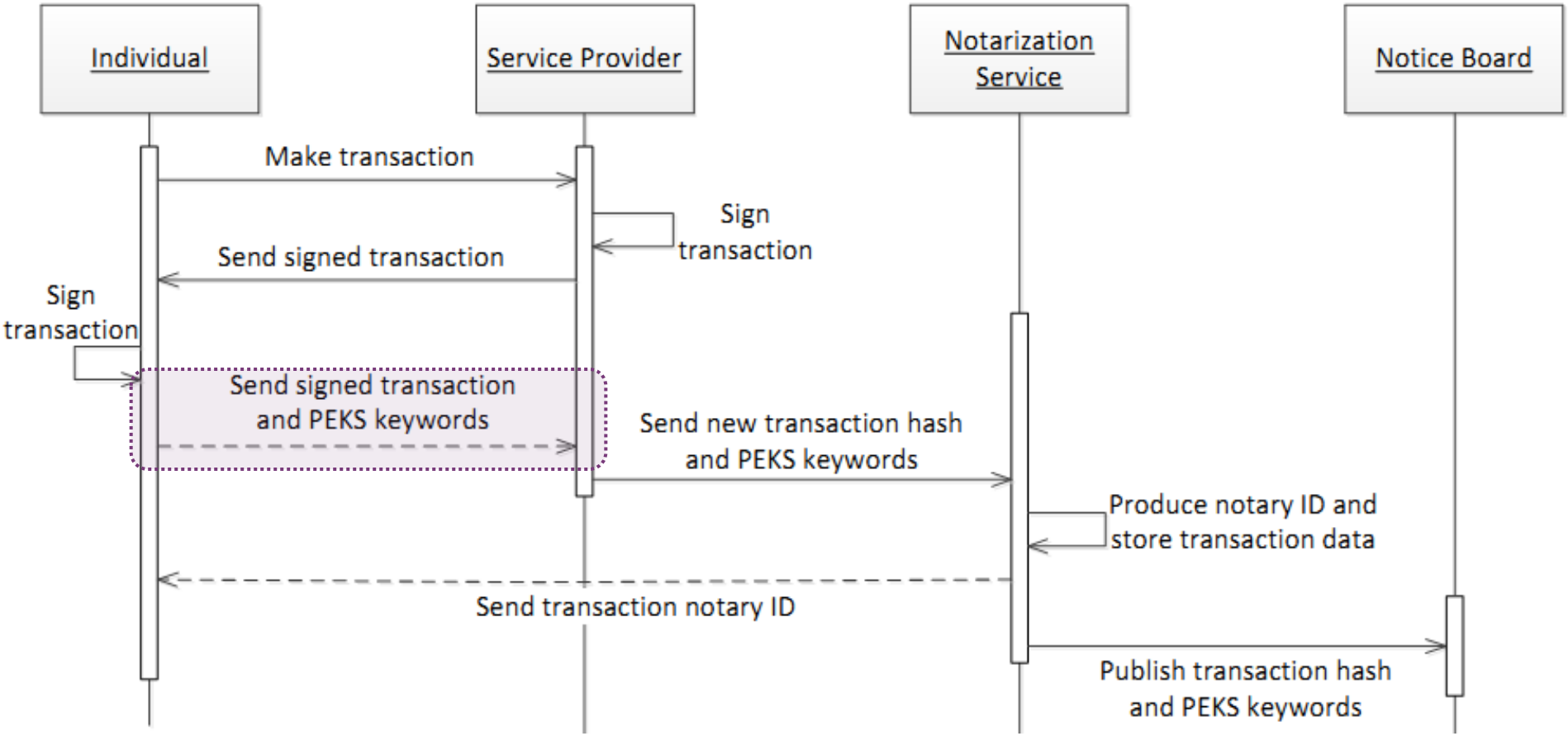
Transaction Insertion Protocol



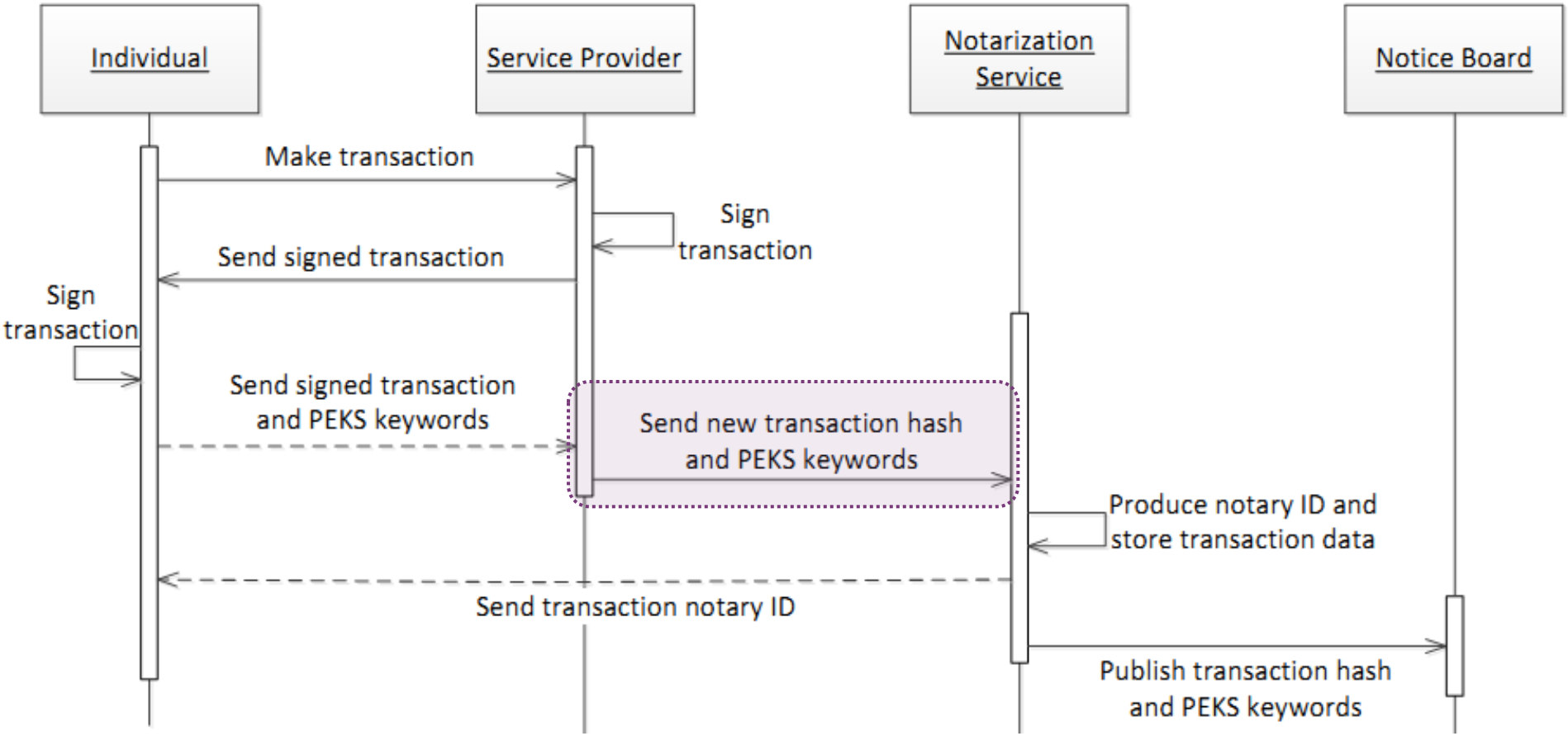
Transaction Insertion Protocol



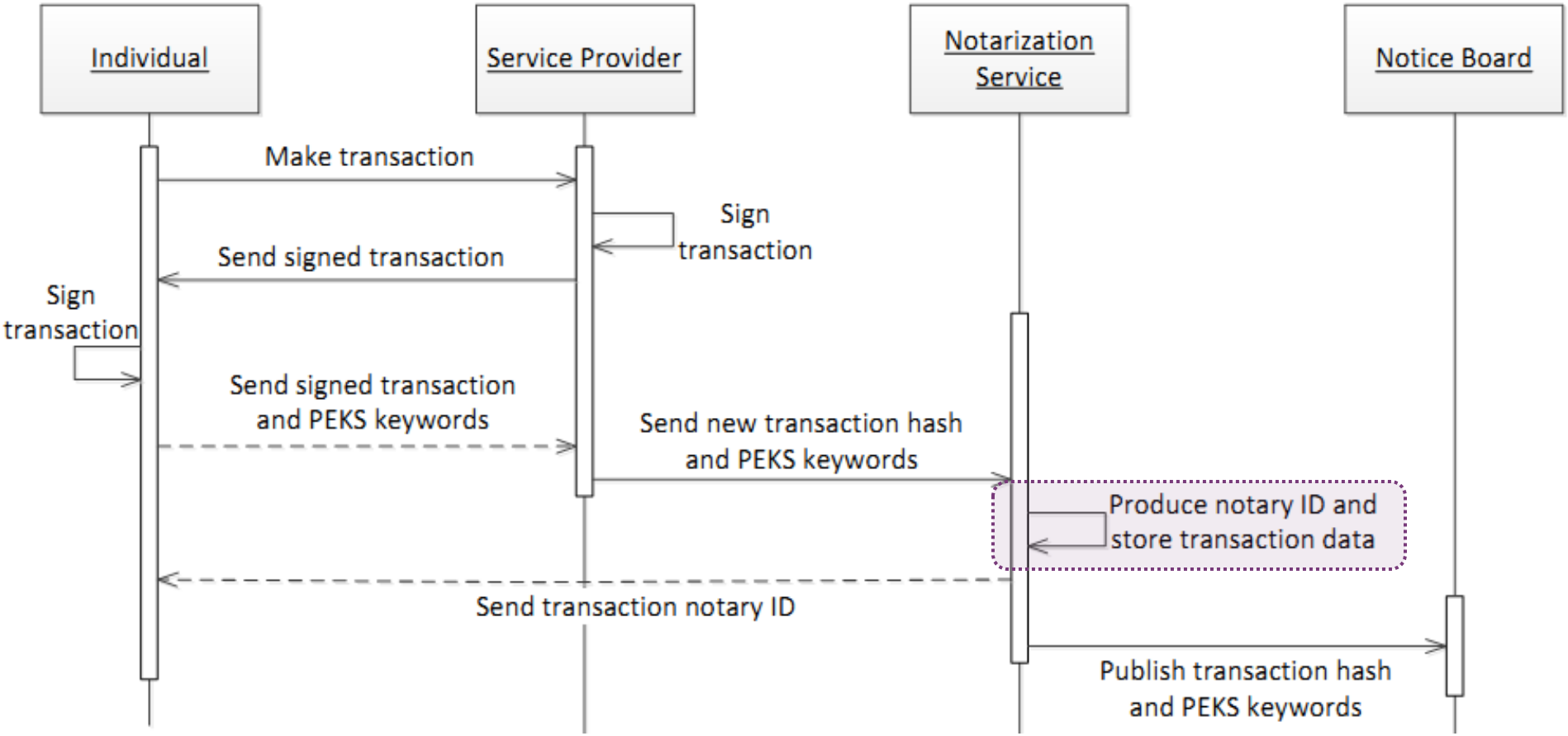
Transaction Insertion Protocol



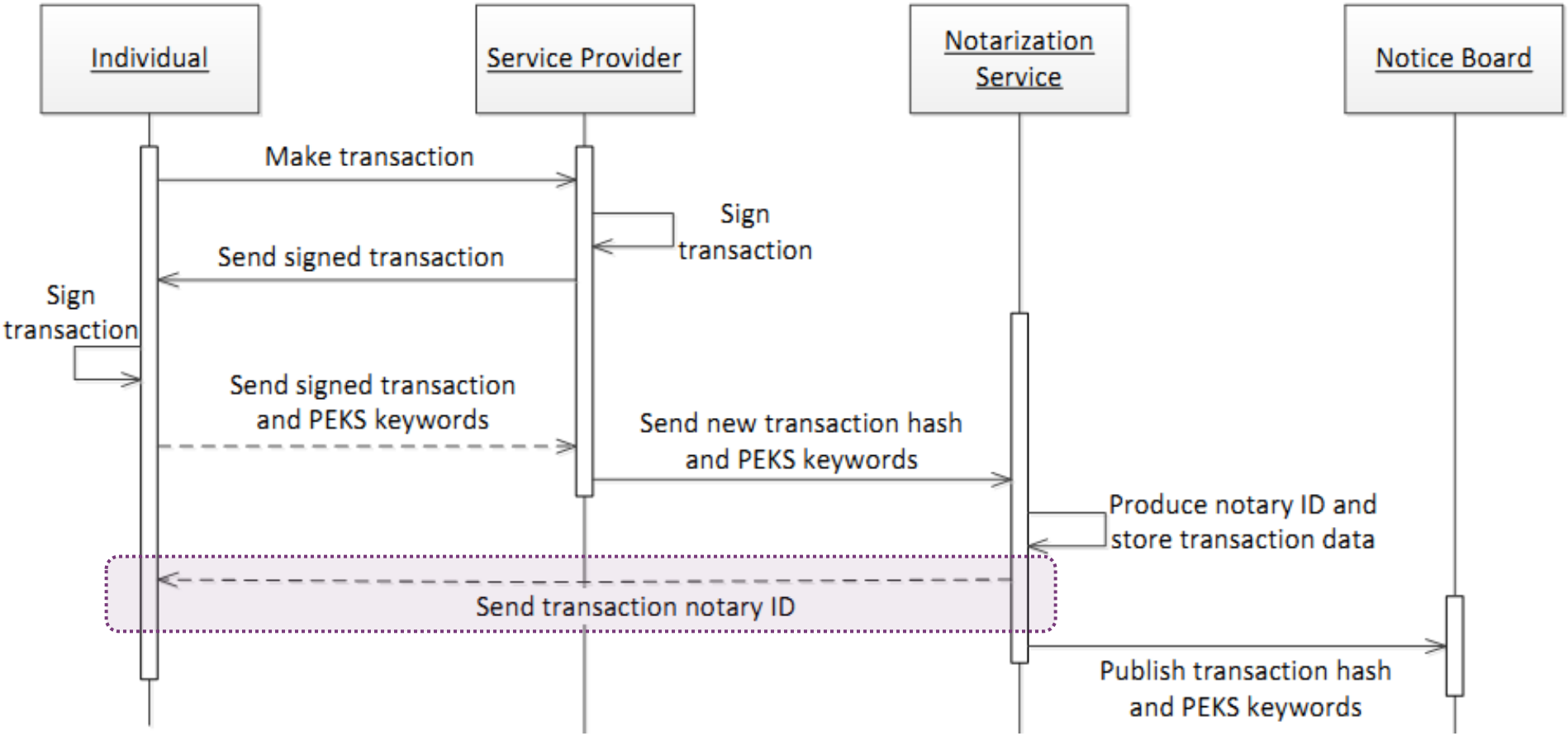
Transaction Insertion Protocol



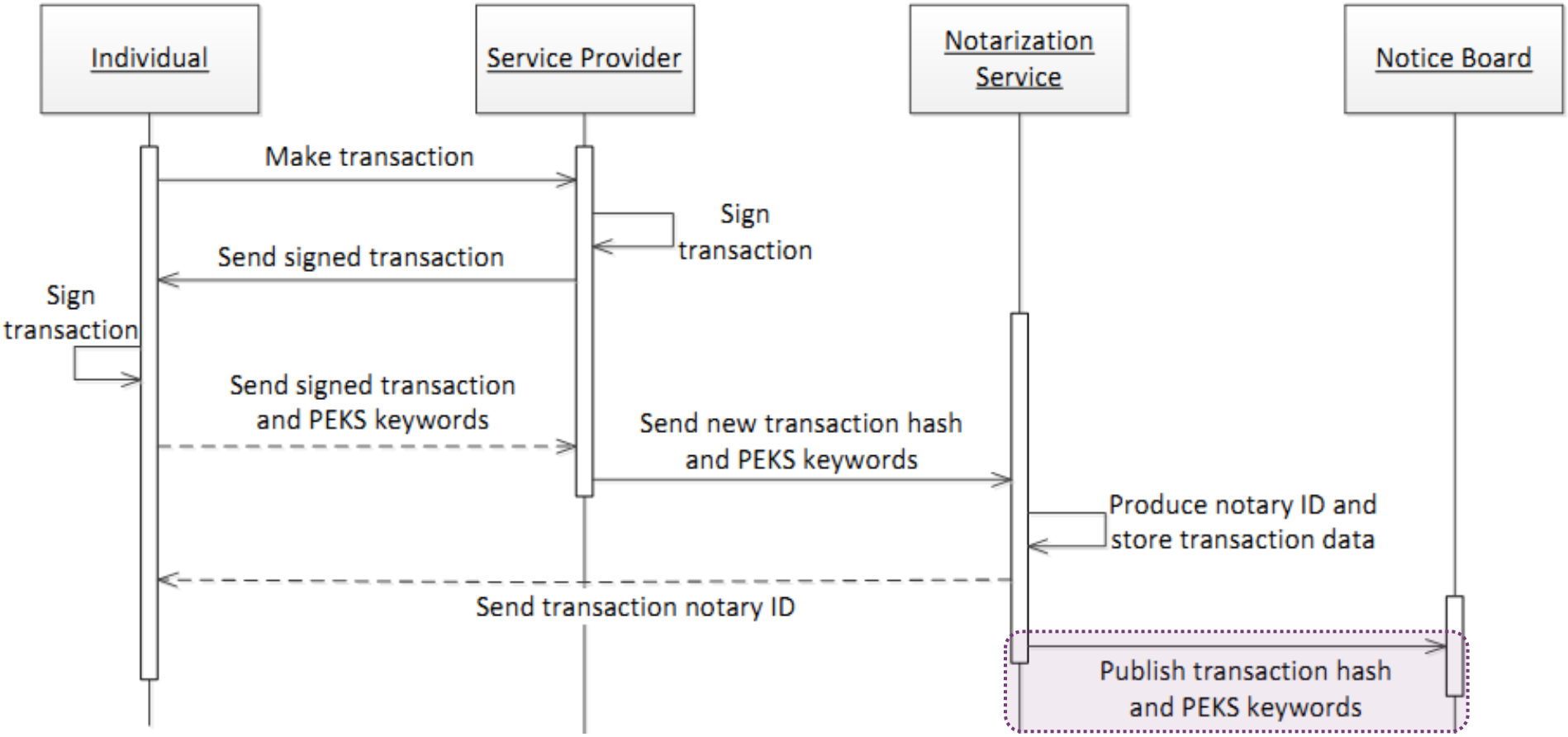
Transaction Insertion Protocol



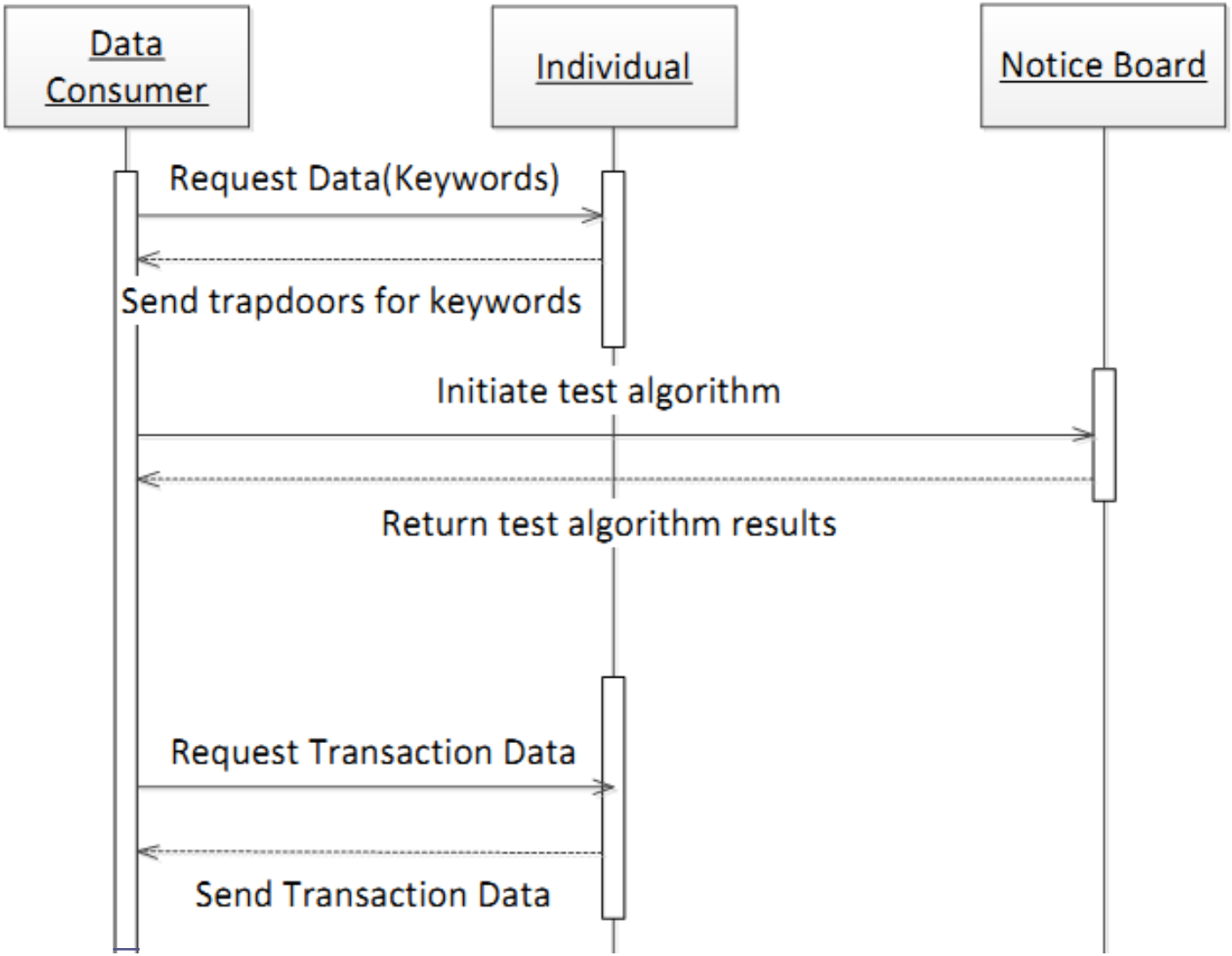
Transaction Insertion Protocol



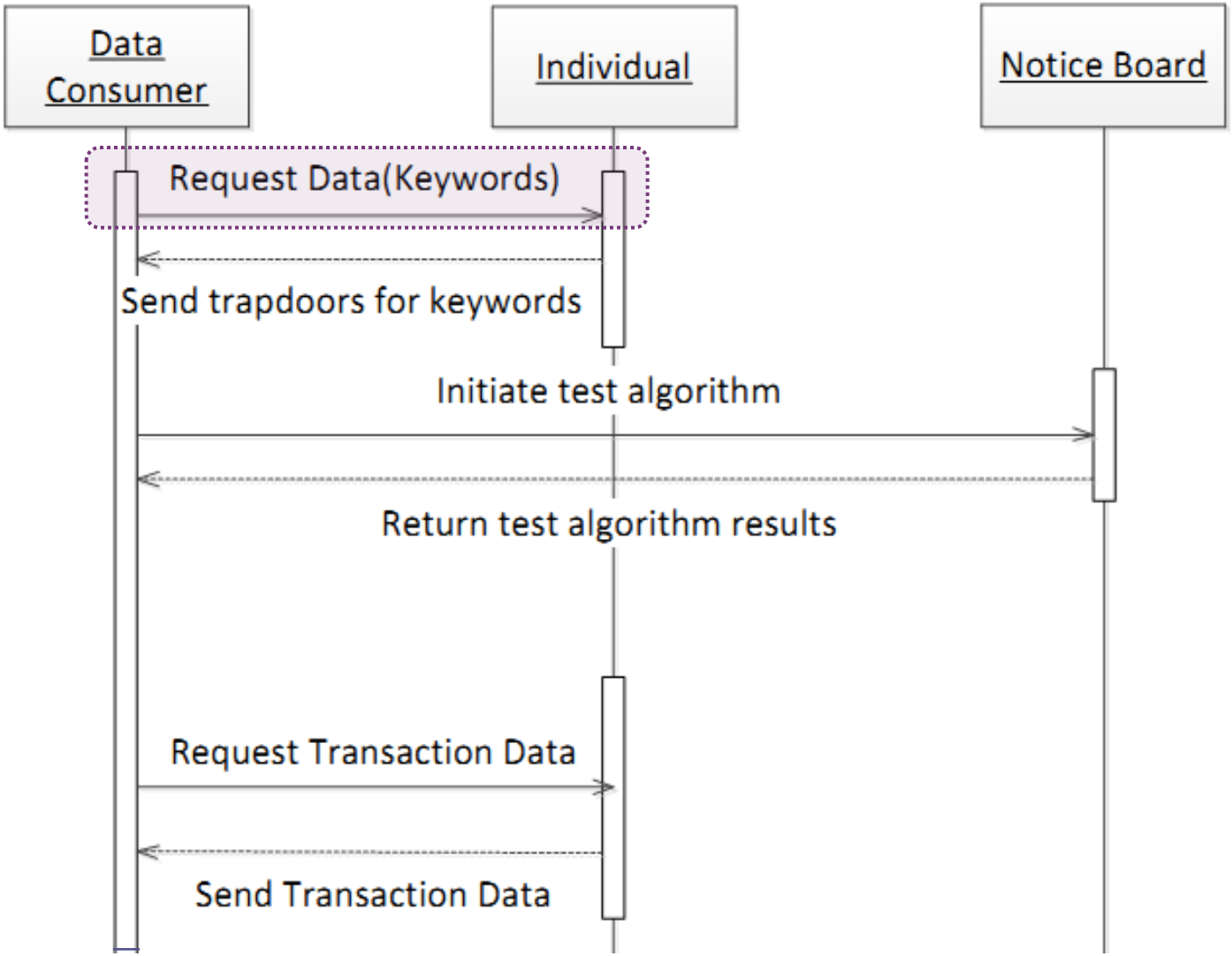
Transaction Insertion Protocol



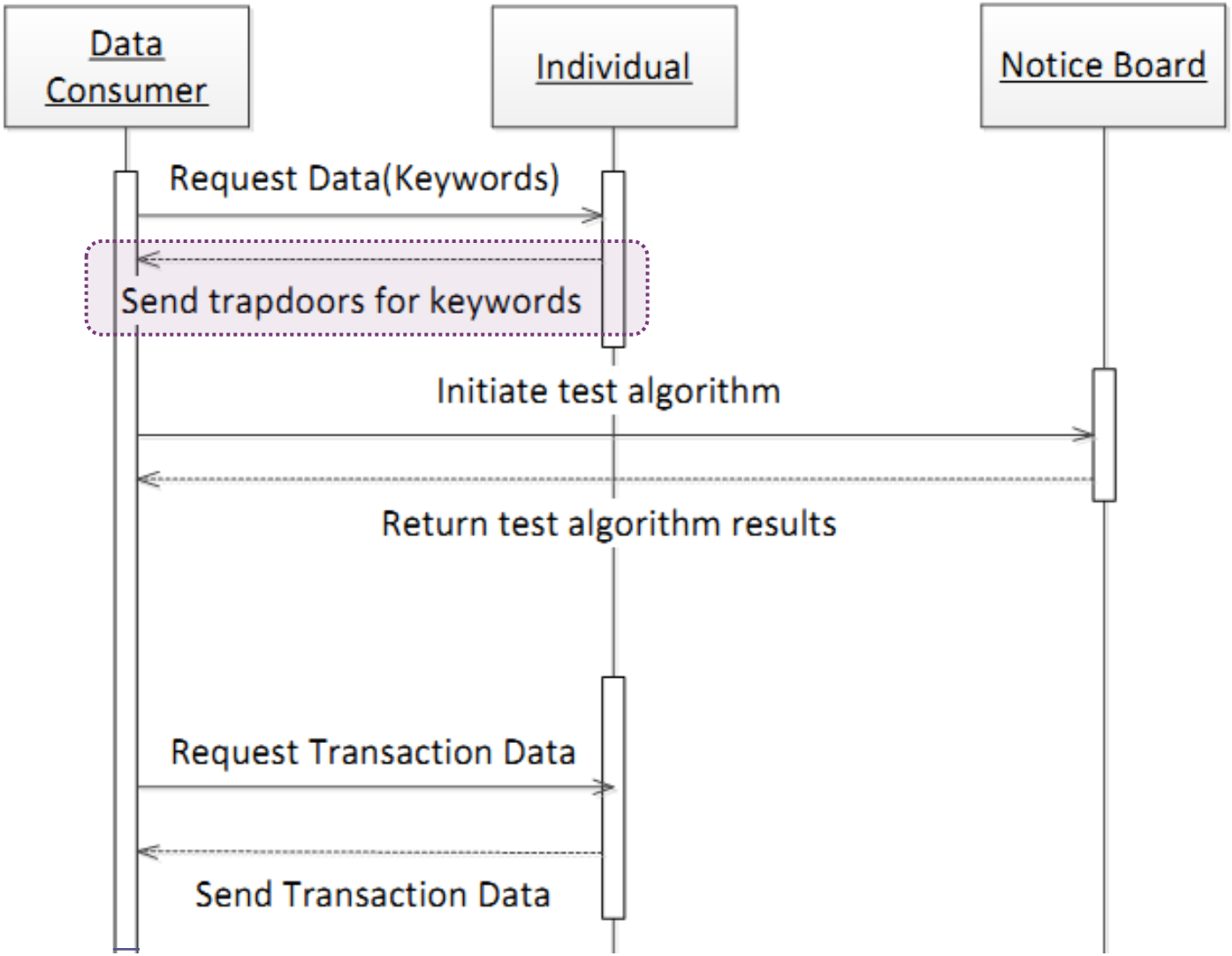
Data Retrieval Protocol



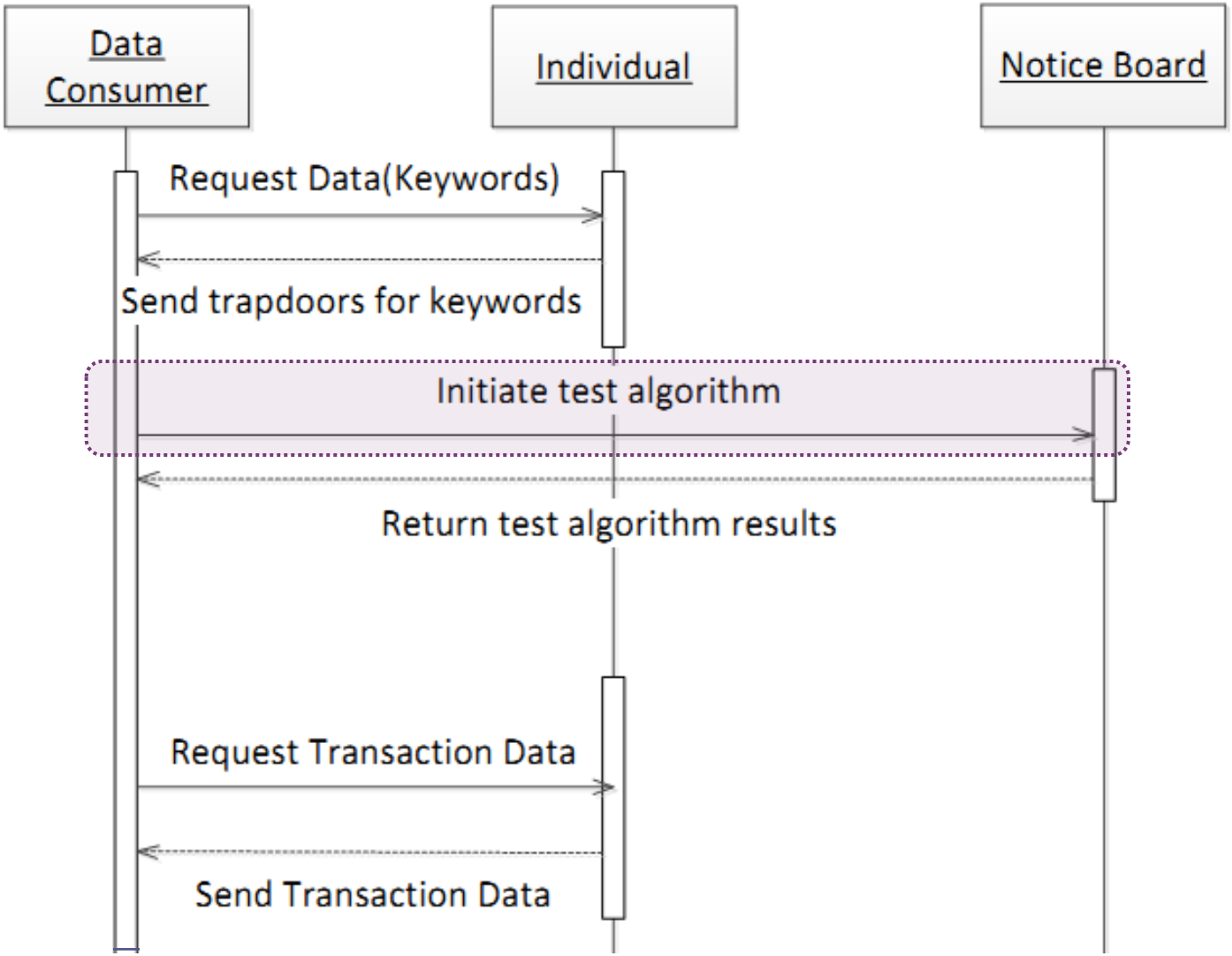
Data Retrieval Protocol



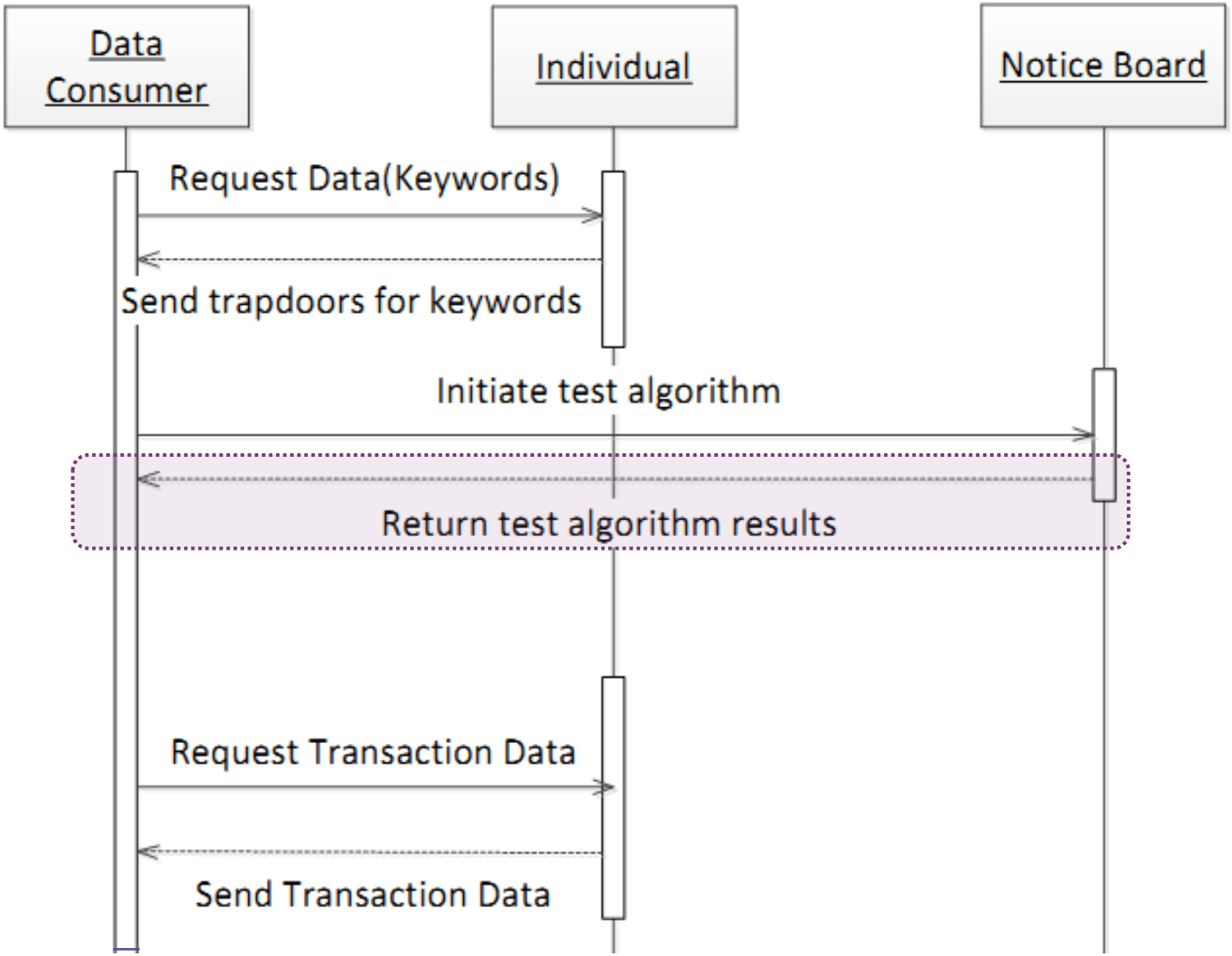
Data Retrieval Protocol



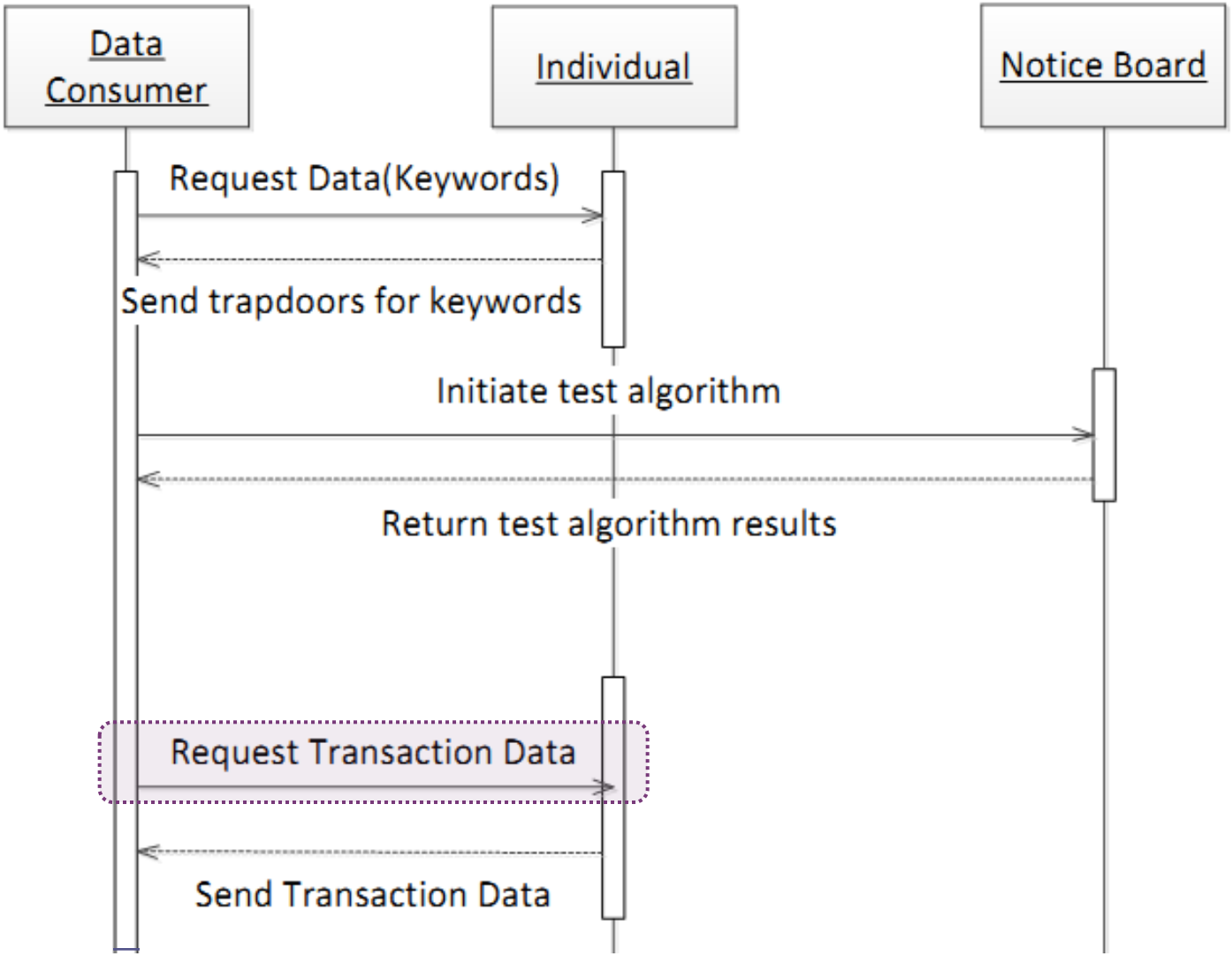
Data Retrieval Protocol



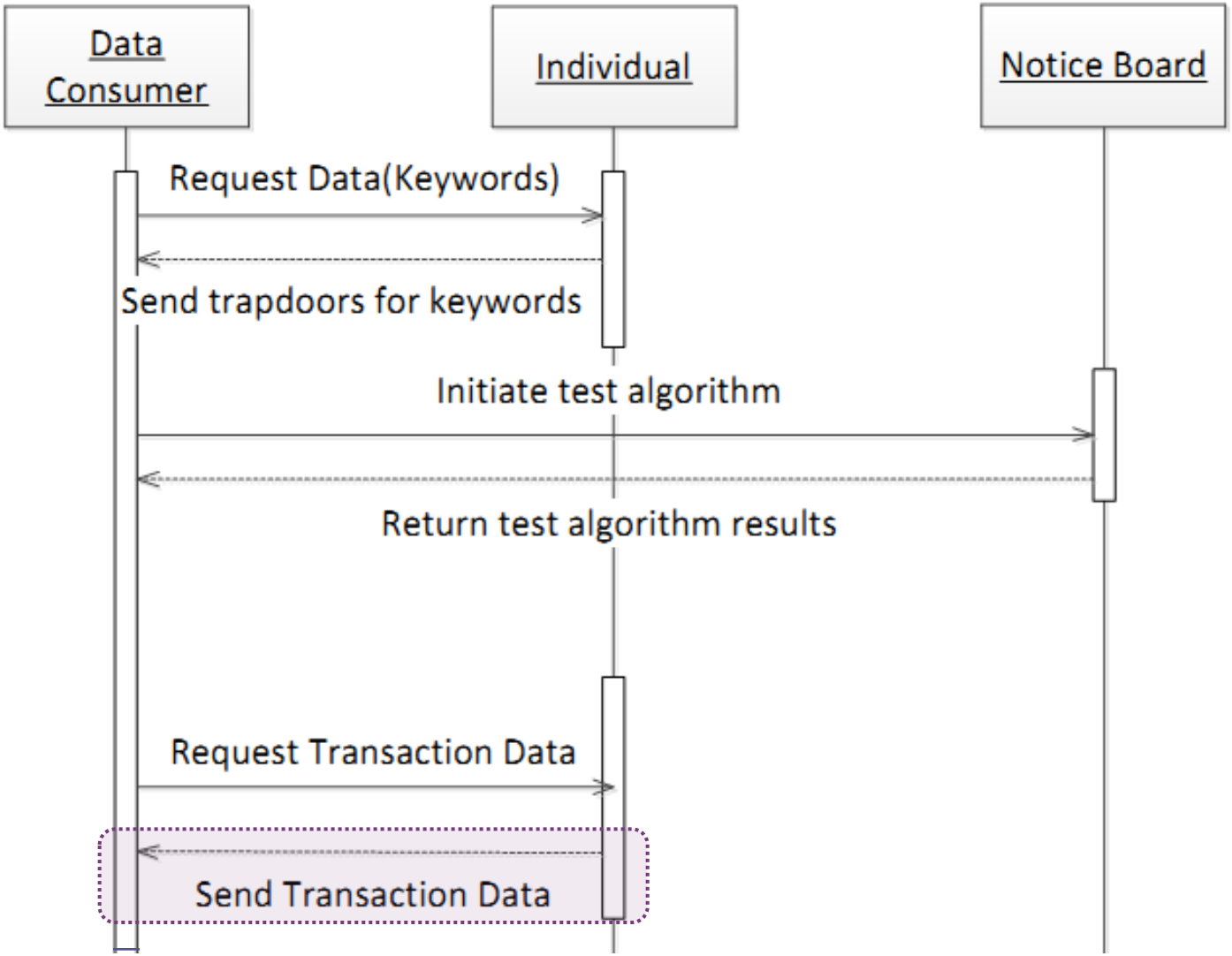
Data Retrieval Protocol



Data Retrieval Protocol



Data Retrieval Protocol



The Portfolio approach

Applications

Portfolio applications

- Tax records.
- Health records.
- Biographic records and e-identities.
- Opinion records for statistics and polls.
- Common requirements:
  - Private **information protection**.
  - **Efficient** and **accountable access** to the portfolio data **for legitimate users**.
  - **Strong accountability**, prohibiting tampering with the portfolio data.

Conclusions

Conclusions

- We propose moving the control of the transaction profile to the customer.
- Today's paradigm can change:
  - Availability of contemporary cryptographic techniques.
  - Increased data protection.
  - Trustworthy utilization of transaction data.
  - Usable with the existing common infrastructure.
- The proposed system is constructed from **existing** and **efficient building blocks**, therefore we believe that it will be **adequately efficient**.

Future work

Future work

- Determining the specifics of the portfolio functionality:
  - Threat model.
  - Implementing a prototype or simulation.
  - Portfolio protocols could be further enhanced and expanded.
- Possible extensions:
  - Support of distributed computations directly by the portfolio agent.
  - Introducing the portfolio into the Cloud.

Thank you!

Algorithms and Privacy Research Unit : euclid.ee.duth.gr

A. Tasidou:
atasidou@ee.duth.gr
utopia.duth.gr/~atasidou
P.S. Efraimidis:
pefraimi@ee.duth.gr
utopia.duth.gr/~pefraimi