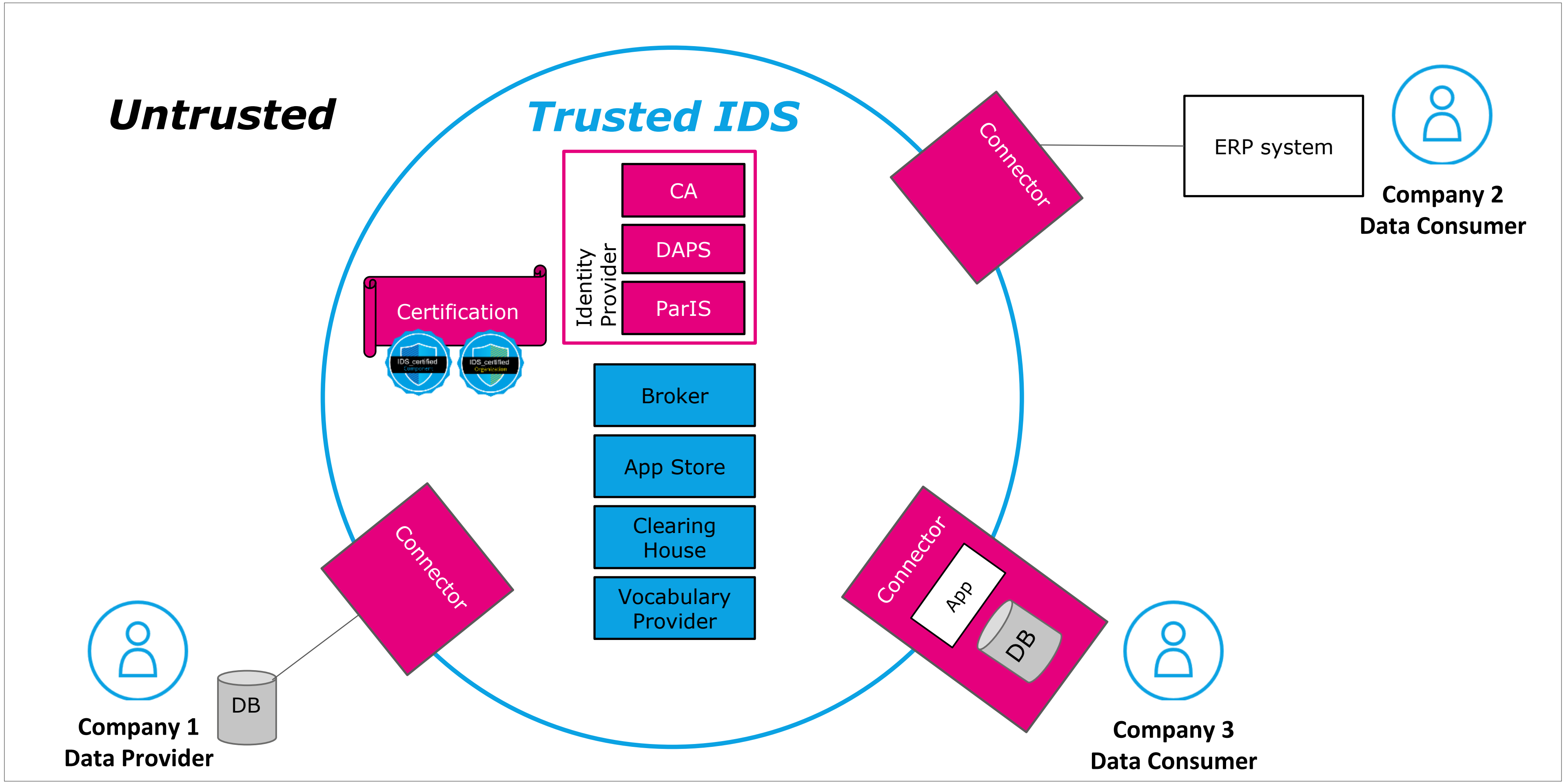
IDS-based Data Spaces

INTERNATIONAL DATA SPACES ASSOCIATION

Overview



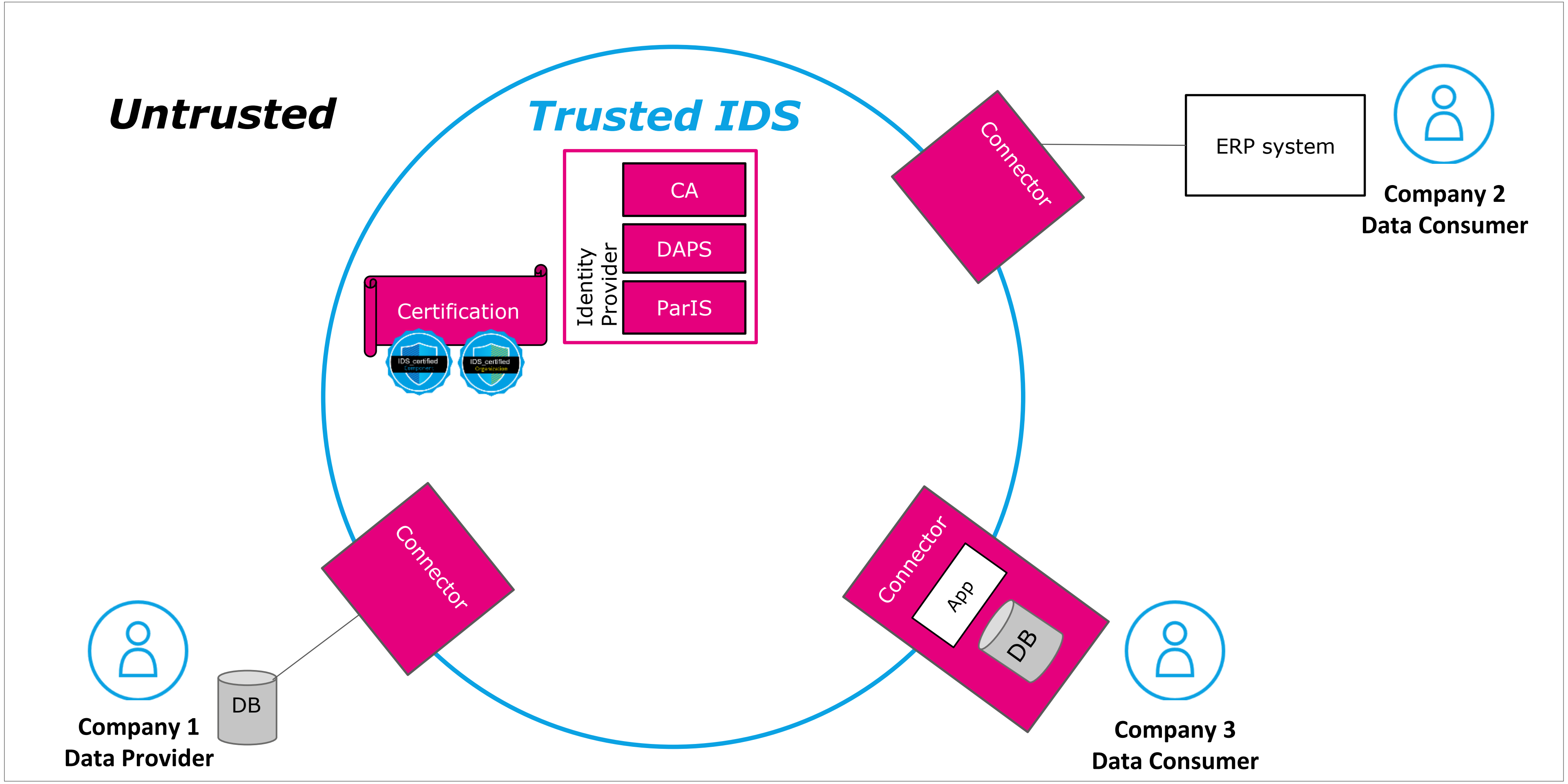
MANDATORY

OPTIONAL

An IDS-based Data Space consists of connectors via which data providers and data consumers are connected to the data spaces and infrastructure components. From a technical perspective some of these components are optional, even though they provide significant functionality without which a data space would not be attractive from a participants perspective, e. g., searching for data endpoints or applications.

IDS-based Data Spaces

Minimum Viable Data Space



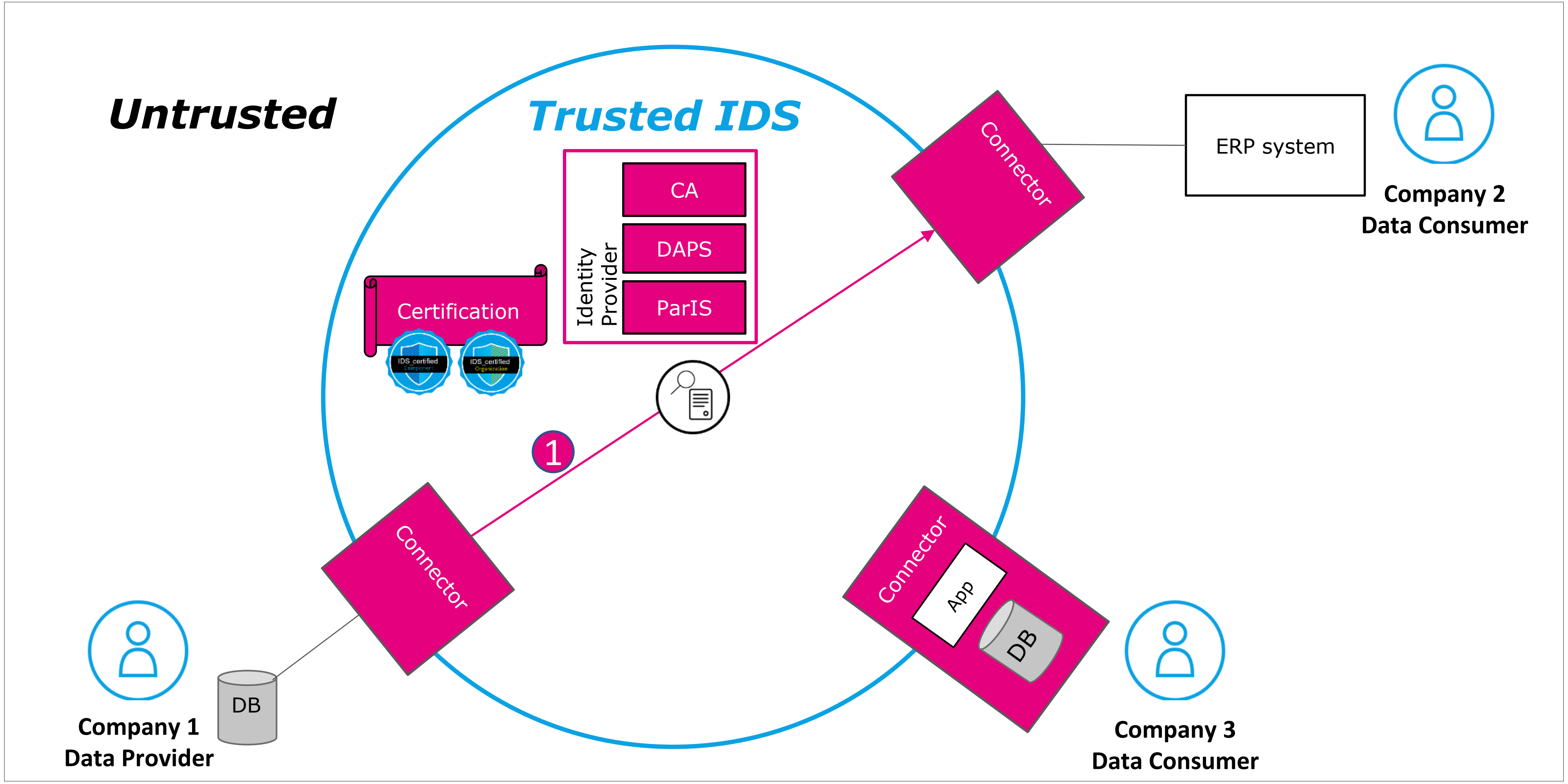
A minimal viable data space consists of 2 or more **IDS connectors** and the **Identity Provider**, which consists of 3 components:

1. The Certificate Authority (**CA**) granting X.509 certificates (not to be confused with certification)
2. The Dynamic Attributes Provisioning Service (**DAPS**) to handle dynamic attributes and manage dynamic access tokens
3. The Participant Information Service (**ParIS**) holding general information of all data space participants

Certification of all components and the operational environments is an additional trust layer, since it ensures the functionality of components work in clearly specified boundaries.

IDS-based Data Spaces

Minimum Viable Data Space – Data Flow



Every **data provider** can define the rules and conditions (usage policies) under which Data is shared with a **data consumer**. These rules include scenarios like, e. g., restriction of data usage for a specific group of participants, restriction of usage to specific purposes, usage of data not more then N times, etc.

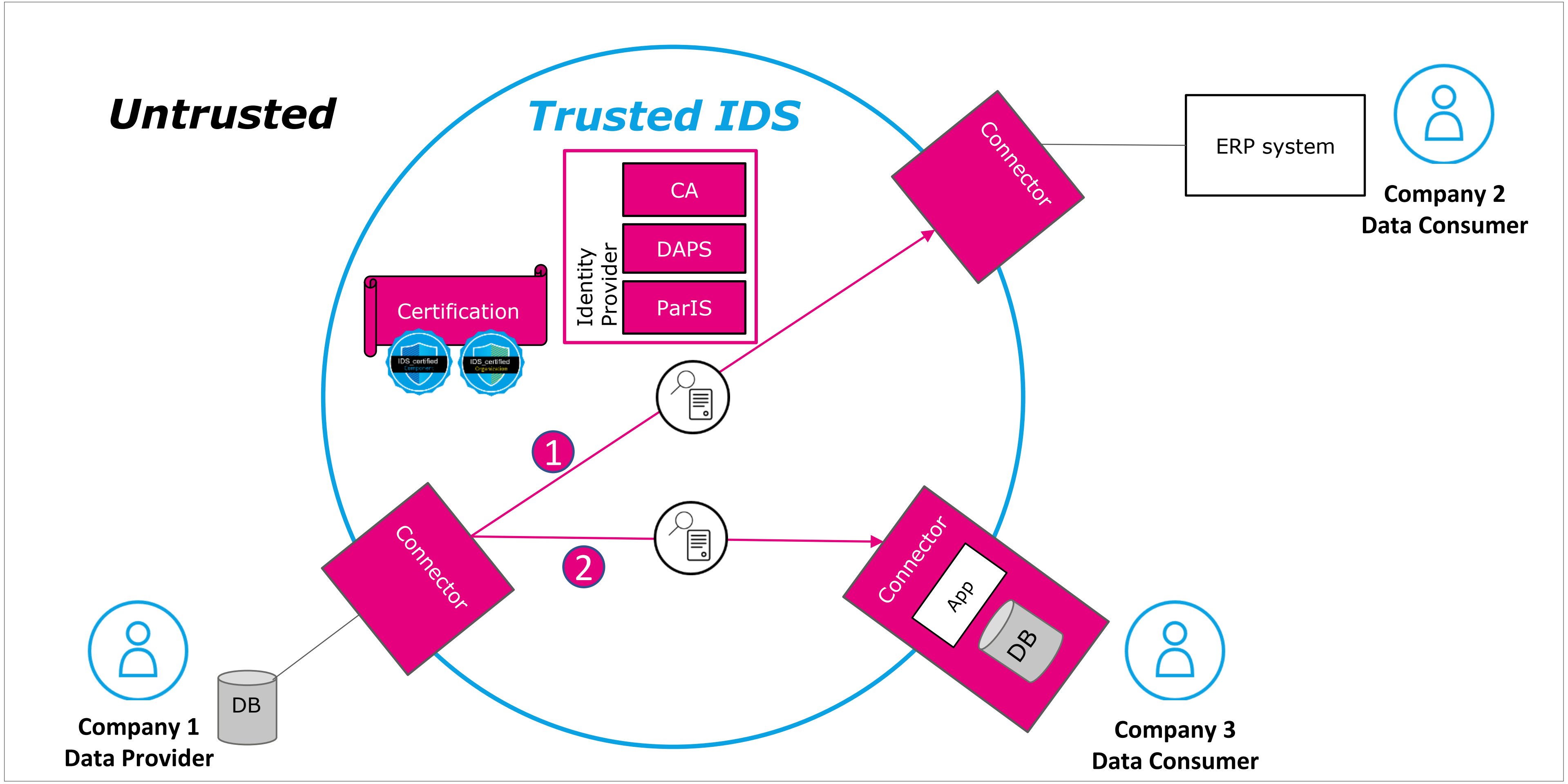
After a data consumer requests a data set from the provider a contract negotiation process is started during which the usage policies are negotiated.

Example 1 (legal enforcement)
The connector of the data consumer (Company 2) is connected with an ERP system that is not deployed in the connector. Therefore the data provider (company 1) has to agree that data will be processed outside of the connector. Here a digital contract between the two parties is establishes that is legally binding for both parties, even though, technical control is lost for the data provider.

IDS-based Data Spaces

INTERNATIONAL DATA SPACES ASSOCIATION

Minimum Viable Data Space – Data Flow



Every **data provider** can define the rules and conditions (usage policies) under which Data is shared with a **data consumer**. These rules include scenarios like, e. g., restriction of data usage for a specific group of participants, restriction of usage to specific purposes, usage of data not more then N times, etc.

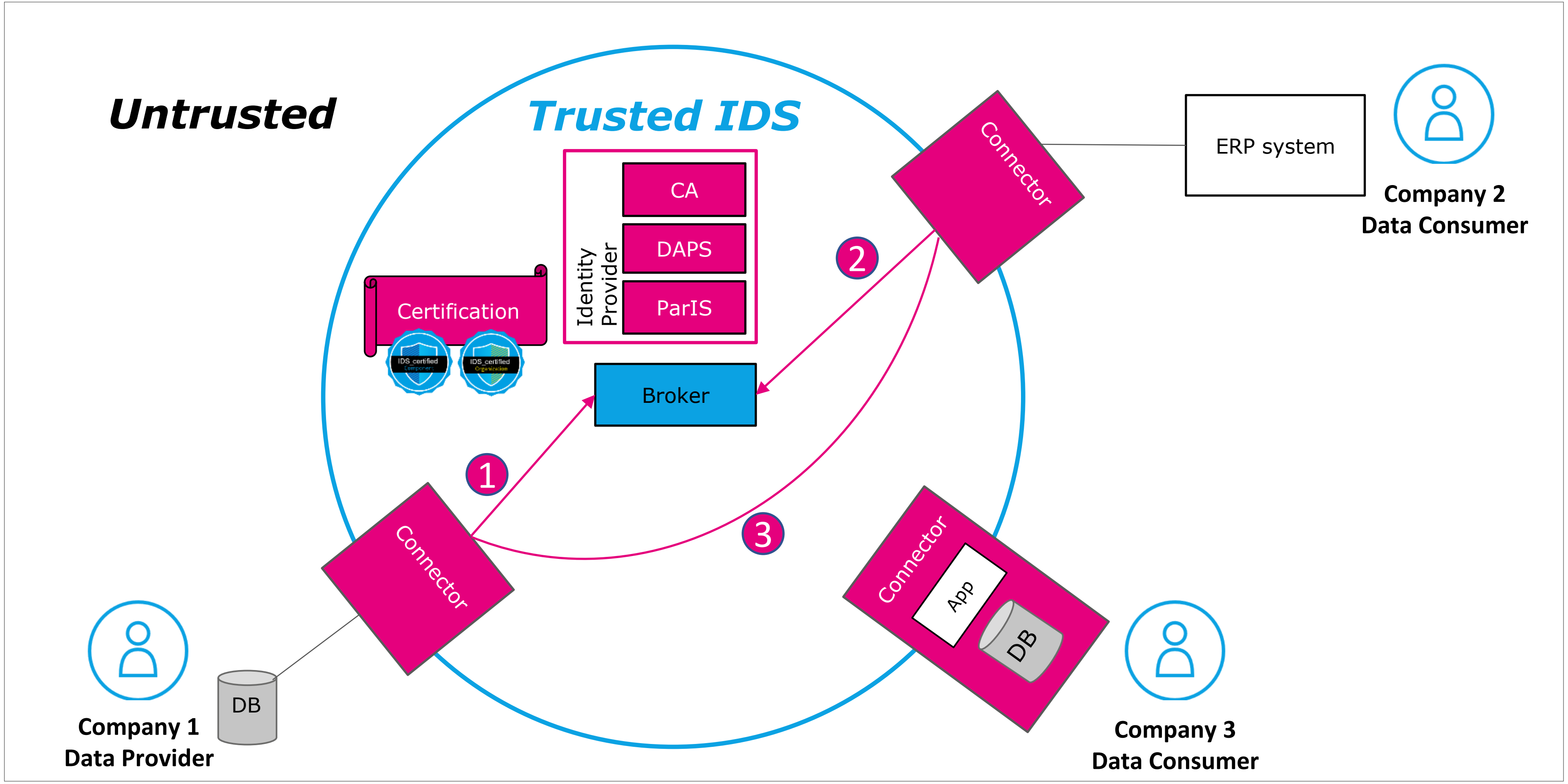
After a data consumer requests a data set from the provider a contract negotiation process is started during which the usage policies are negotiated.

Example 2 (technical enforcement)
The app that is deployed in the connector of the data consumer (company 3). Applications which are deployed in the runtime environment of a connector can enforce usage policies in a technical manner, e. g., deleting data after 5 days.
This adds a further trust layer to the digital contracts as established with company 2.

IDS-based Data Spaces

INTERNATIONAL DATA SPACES ASSOCIATION

Extended Functional Infrastructure - Broker



The **Meta Data Broker** (short Broker) is storing information about the data endpoints offered by participants of the data space. It does not store the data sets itself, but only the meta information. We can compare its function to the one of a search engine.

It is an optional component, because the connection between two participants also can be established directly in case they are known to each other.

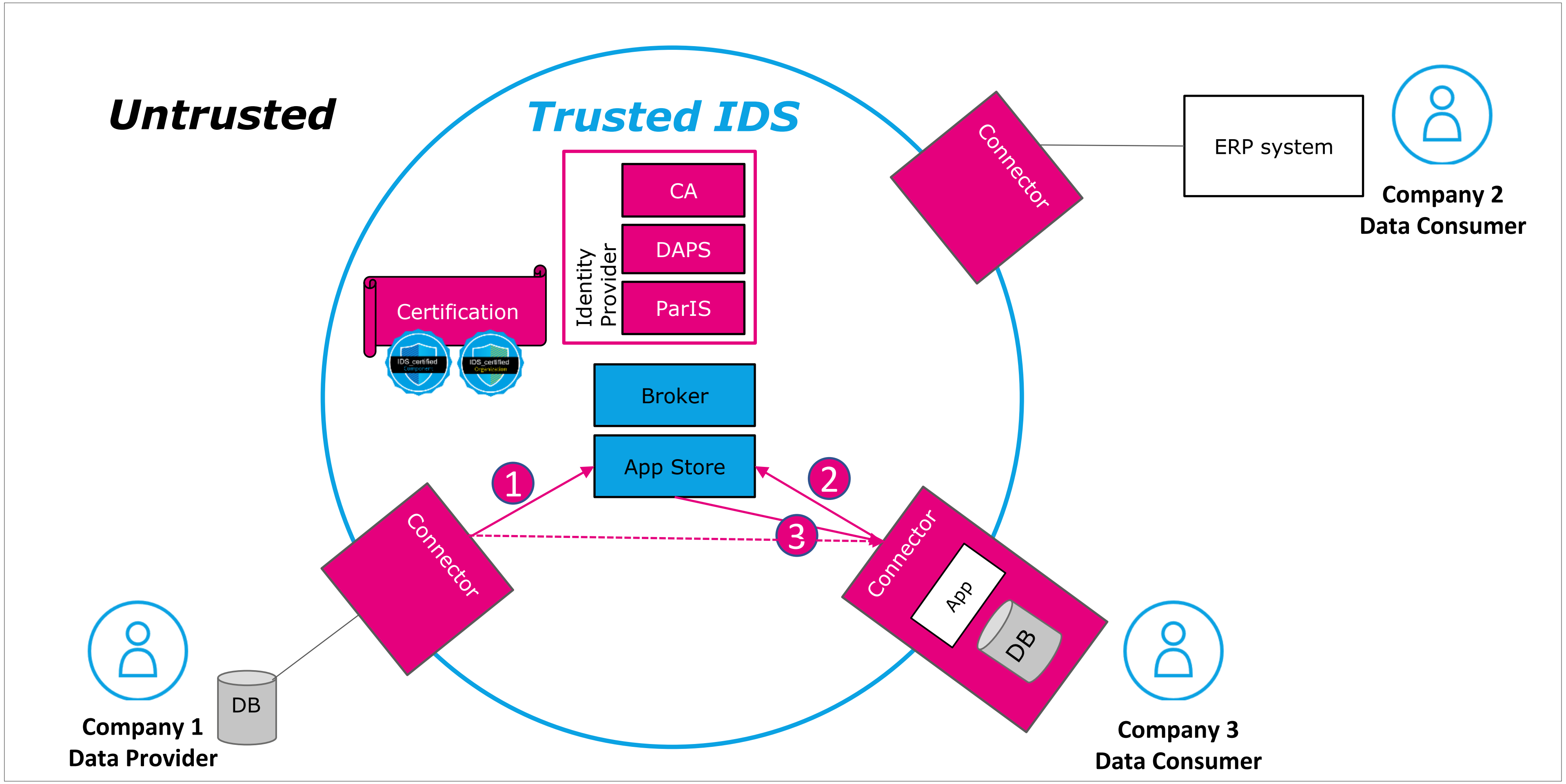
1 Data providers can register their data sets at the broker where the offering will be discoverable.

2 Data consumers can search for data they need for their use case specific purposes.

3 After a successful contract negotiation the data consumer can access the data of the provider.

IDS-based Data Spaces

Extended Functional Infrastructure – App Store



The **App Store** is an infrastructure component where participants can search and discover applications for data transformations which are deployable in their connectors.

1 Participants of the data space can make standard applications visible at the app store.

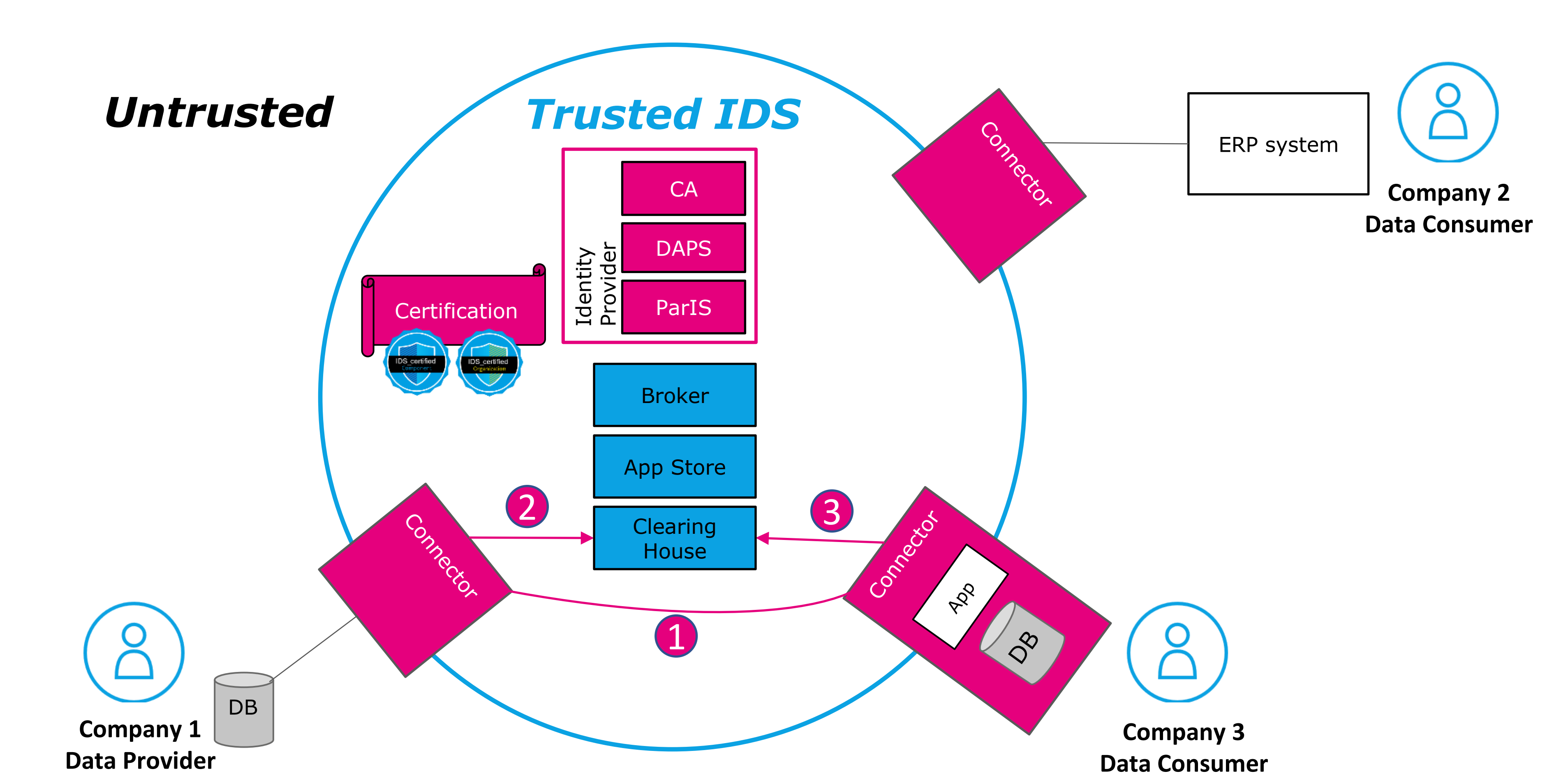
2 Any other participant interested in this functionality is able to discover the app and

3 deploy the app in the connector. The app also can be sourced from the participants who registered the app at the app store.

IDS-based Data Spaces

INTERNATIONAL DATA SPACES ASSOCIATION

Extended Functional Infrastructure – Clearing House



The **Clearing House** at the current state can be understood as a transaction log.

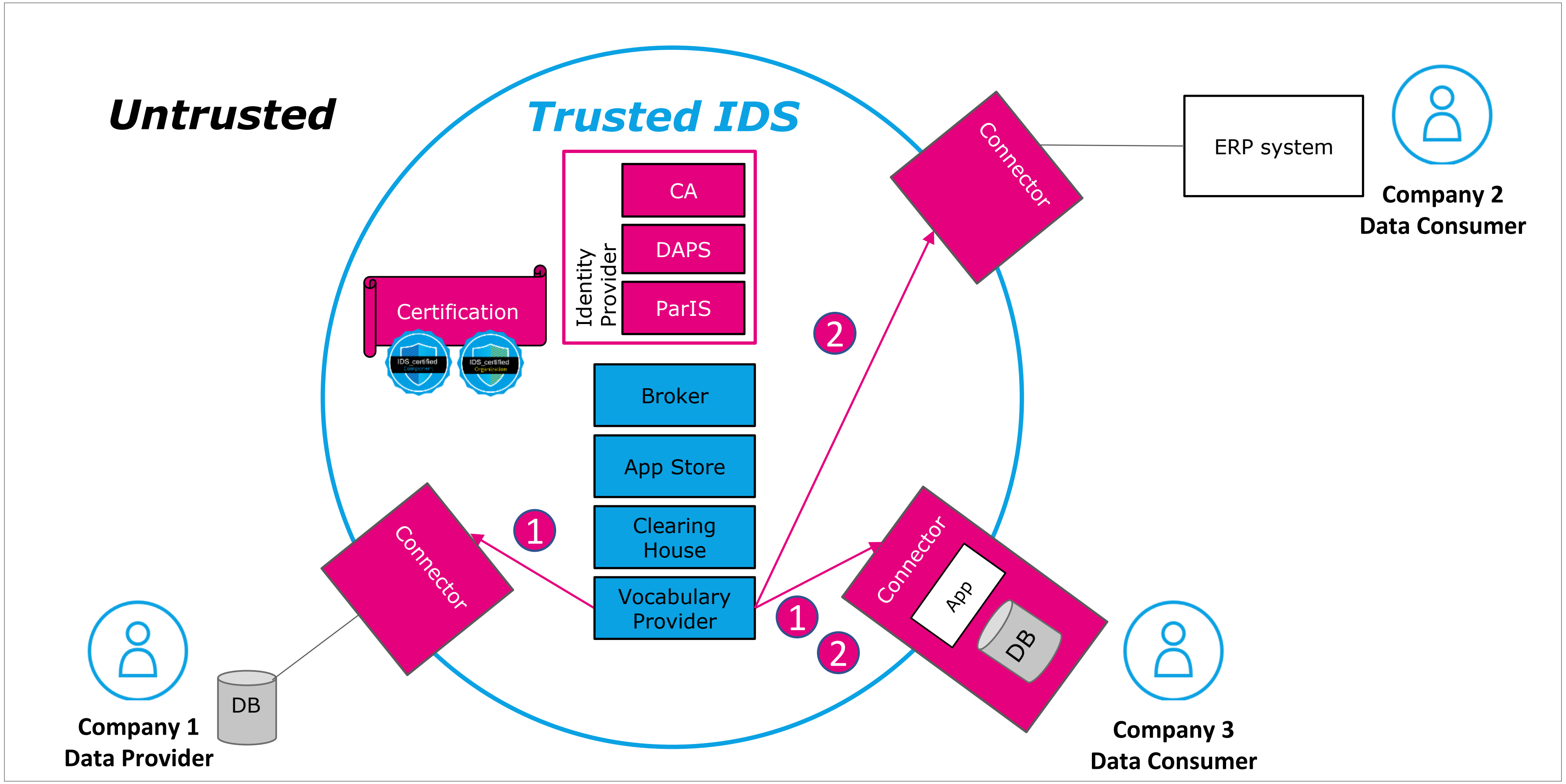
1 In case two participants of the data space exchange data, the Clearing House logs this transaction 2 + 3.

This leads to a higher trustworthiness, since data flow can be proofed by a neutral third party.

It also can be used to establish pay-per-use or better said "pay-per-transfer" business models.

IDS-based Data Spaces

Extended Functional Infrastructure – Clearing House



The **Vocabulary Provider** is the infrastructure component where domain specific vocabularies (ontologies) can be provided to the participant of the data space.