IDENTITY & SECURITY

AUTHORIZATION MODEL FOR JAVASCRIPT USAGE OF HARDWARE BASED KEYS

HBSS Community Group – W3C - 09/06/2016

SAFRAN

The problem

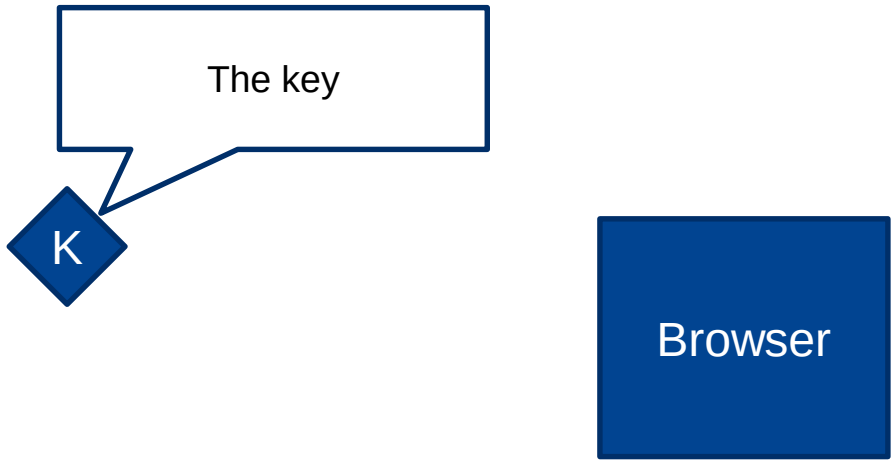
How to manage the right for a web site through its web pages and Javascript to use a key ?

The proposal

Two complementary approaches:

- **Browser based**
- **Key issuer based**

Browser based approach - The parties

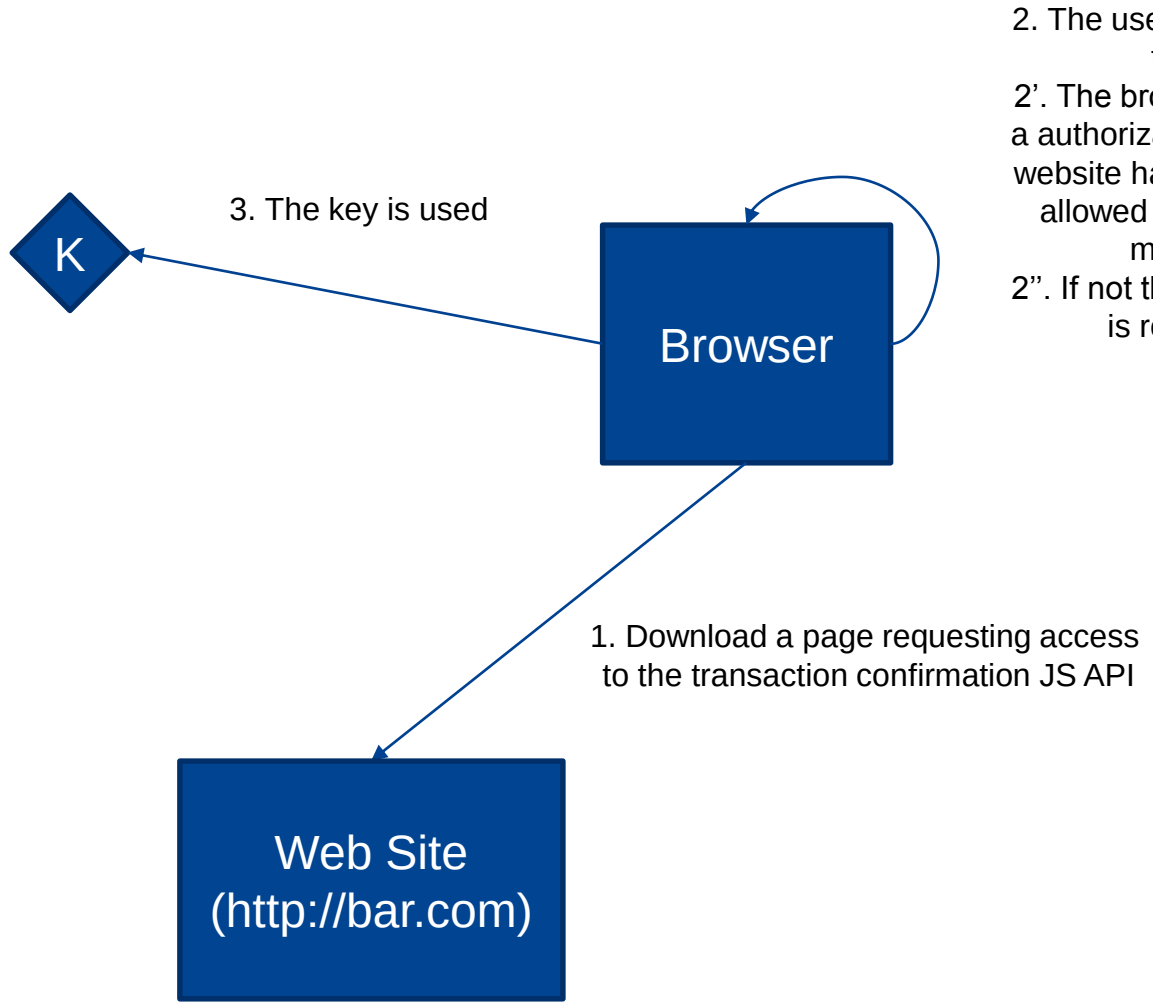


The parties

The web site: the party that is requesting access to the key

The browser: the user browser that is in charge of controlling Javascript access to the key

Browser based approach - Using a certificate

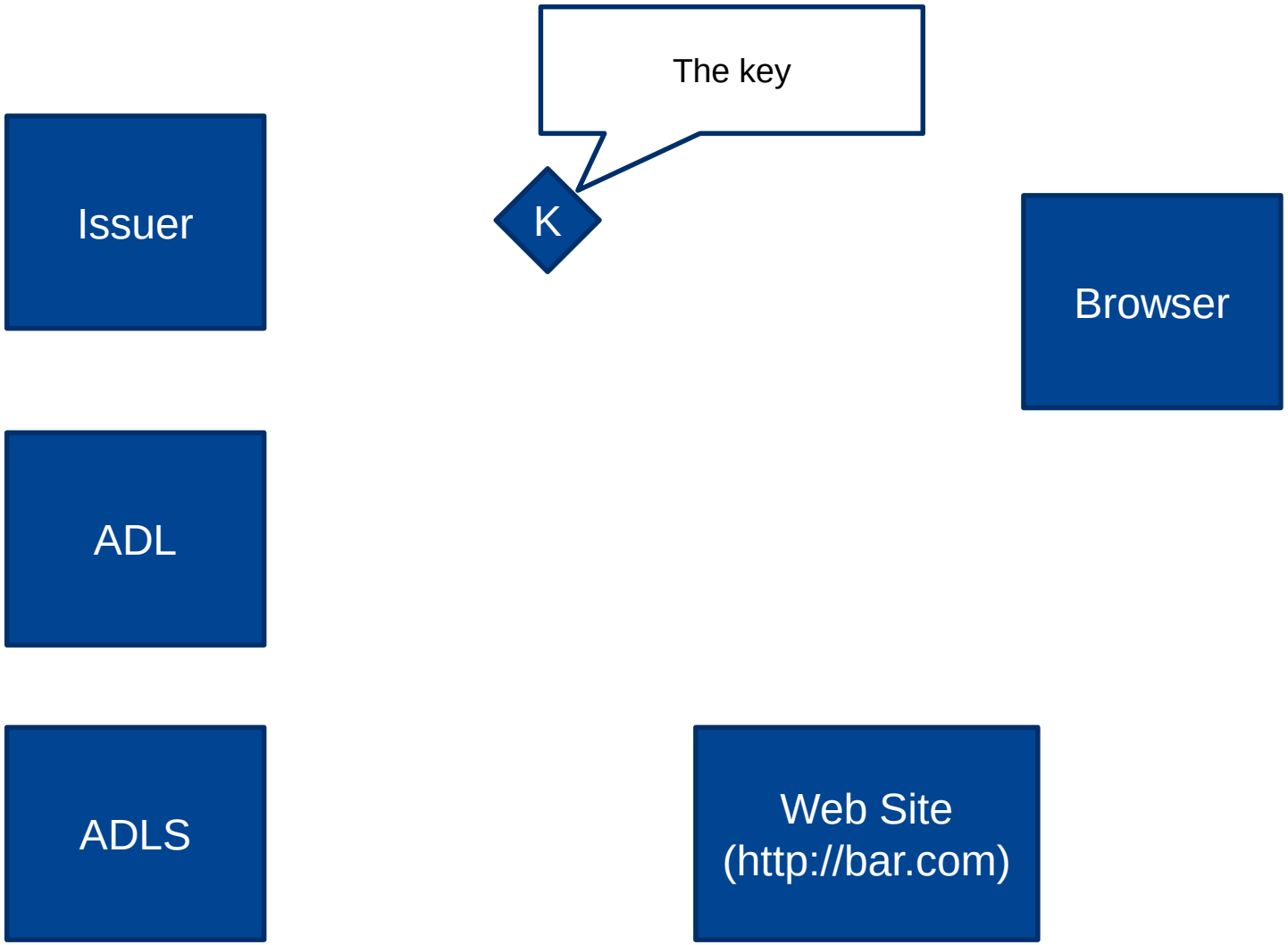


The proposal

Two complementary approaches:

- **Browser based**
- **Key issuer based**

Key issuer based - The parties



Key issuer based - The parties

The issuer: the issuer of the key

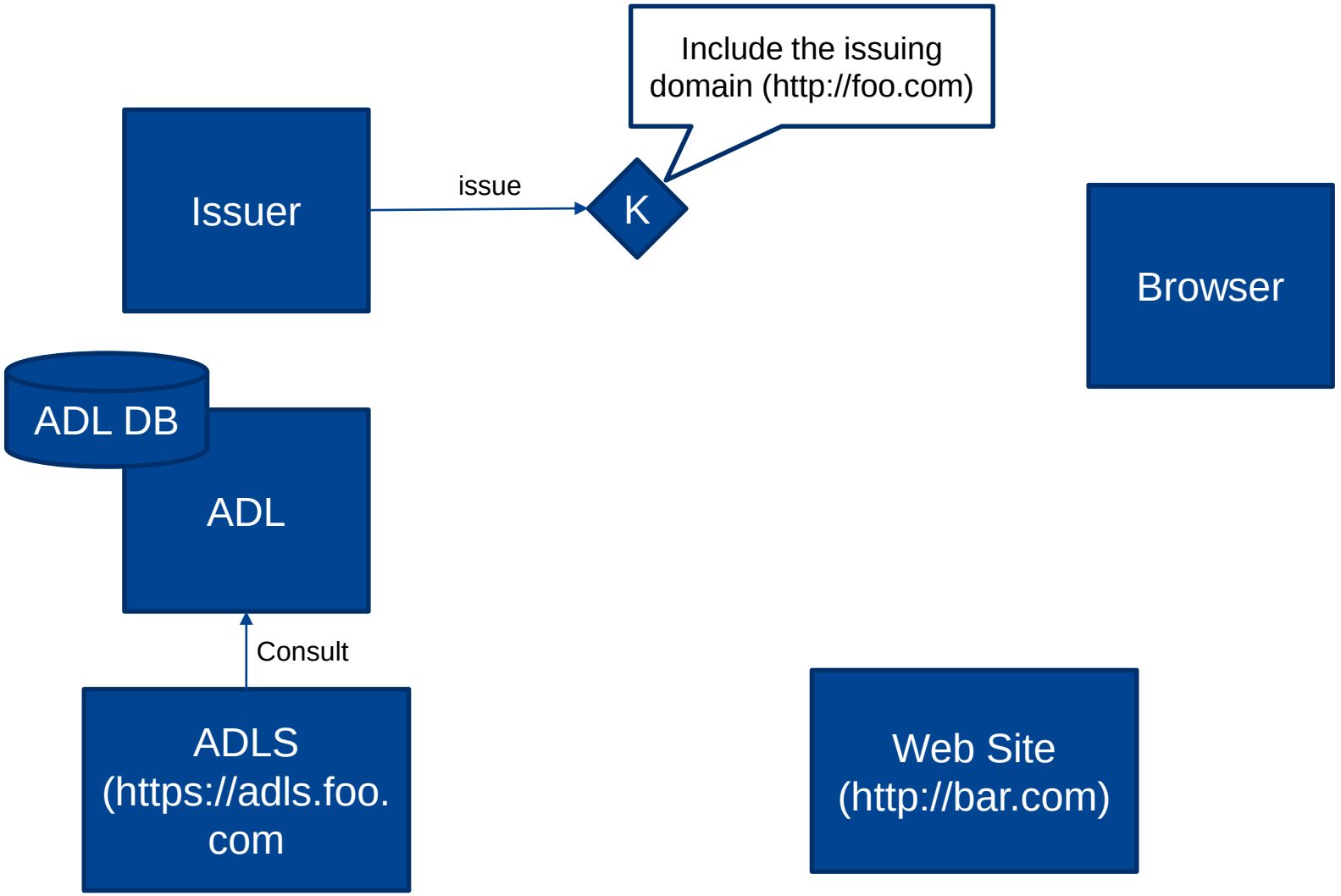
The authorized domain list: a global, scoped or per-user list of authorized domain lists to use the key

The authorized domain list service: a service that provides that checks

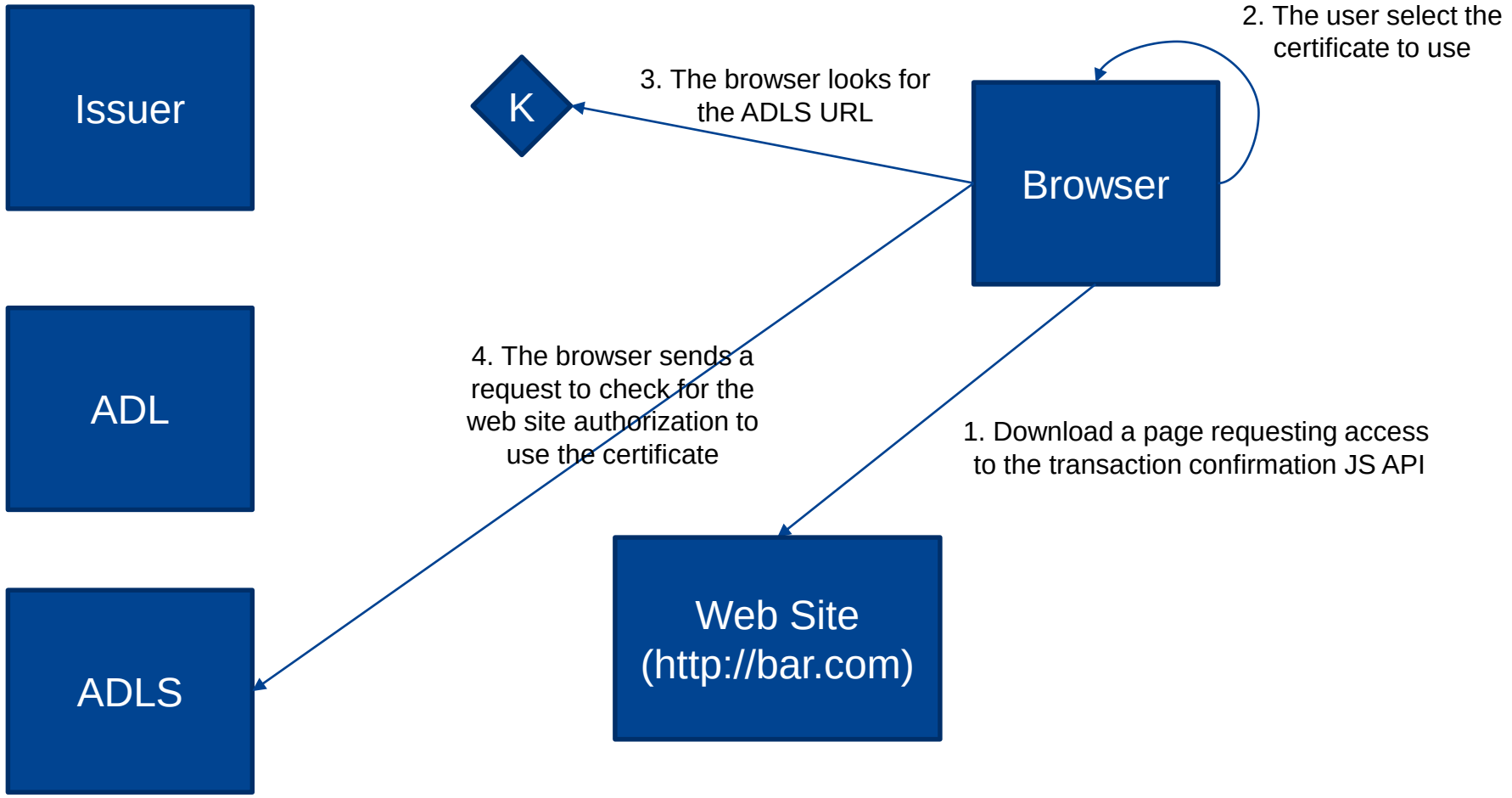
The web site: the party that is requesting access to the key

The browser: the user browser that is in charge of controlling Javascript access to the key

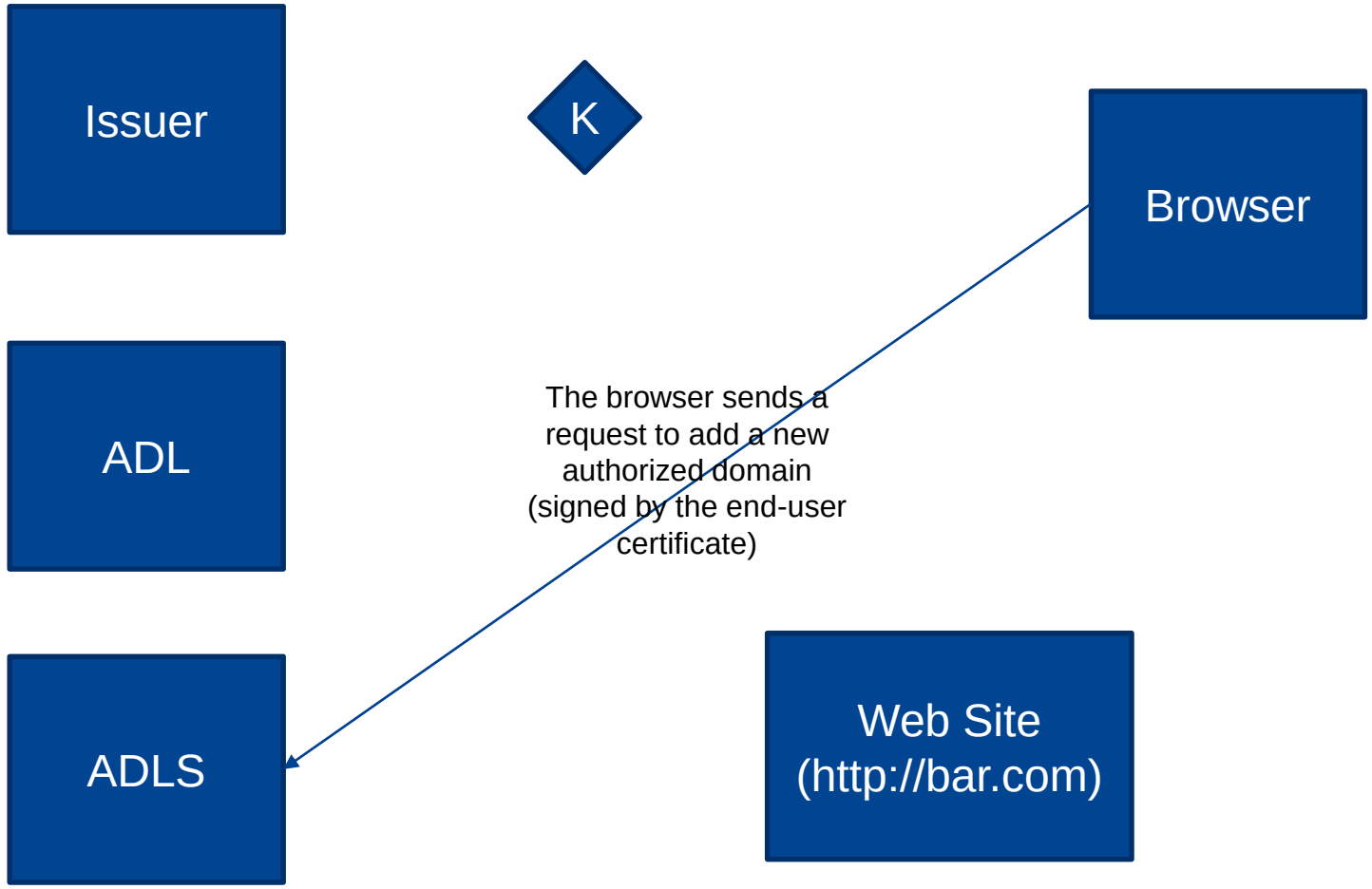
Key issuer based - Issuing a certificate



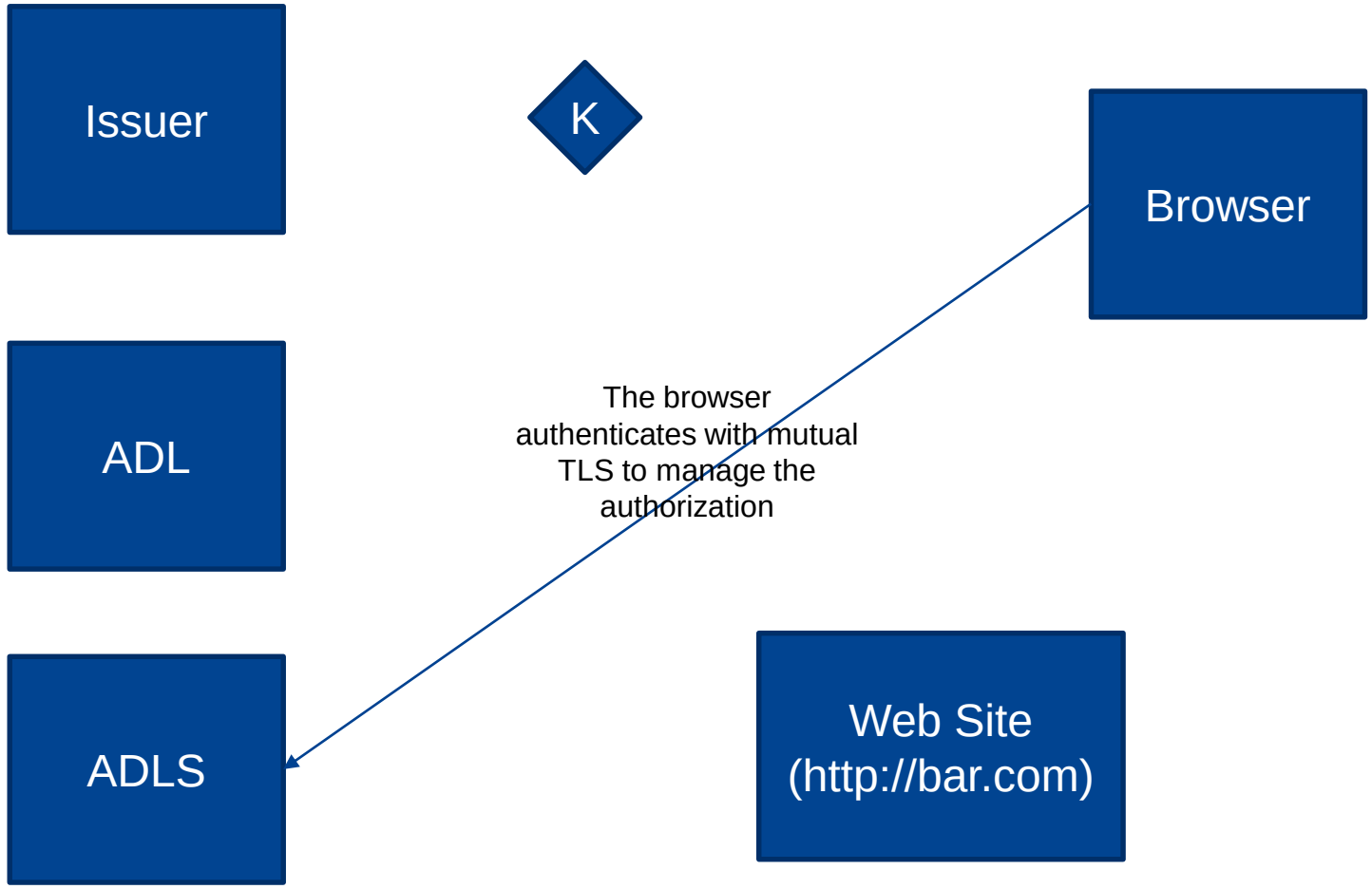
Key issuer based approach - Using a certificate



Key issuer based approach - The user adds a new authorized domain (optional)



Key issuer based approach - The user manages his/her authorizations (optional)



Key issuer based approach - Hypothesis

The ADLS URL is in the issuer definition (CA policy)

The ADLS URL is public

The ADLS can:

- **Enforce a white list of authorized domains**
- **Enforce a black list of rejected domains**
- **Allow (or not) the user manages his/her own private lists by adding/removing domains**

Key issuer based - Identified issues

- **How guarantee the privacy of the end-user ?**