



Platform Independent Token Based Authentication for Web Services

A focus on the user side component of an authentication framework
using Trustbearer Live and Oberthur ID-One Cosmo cards

by Yann Bouan
Technical Director
Oberthur Technologies – Identity Division



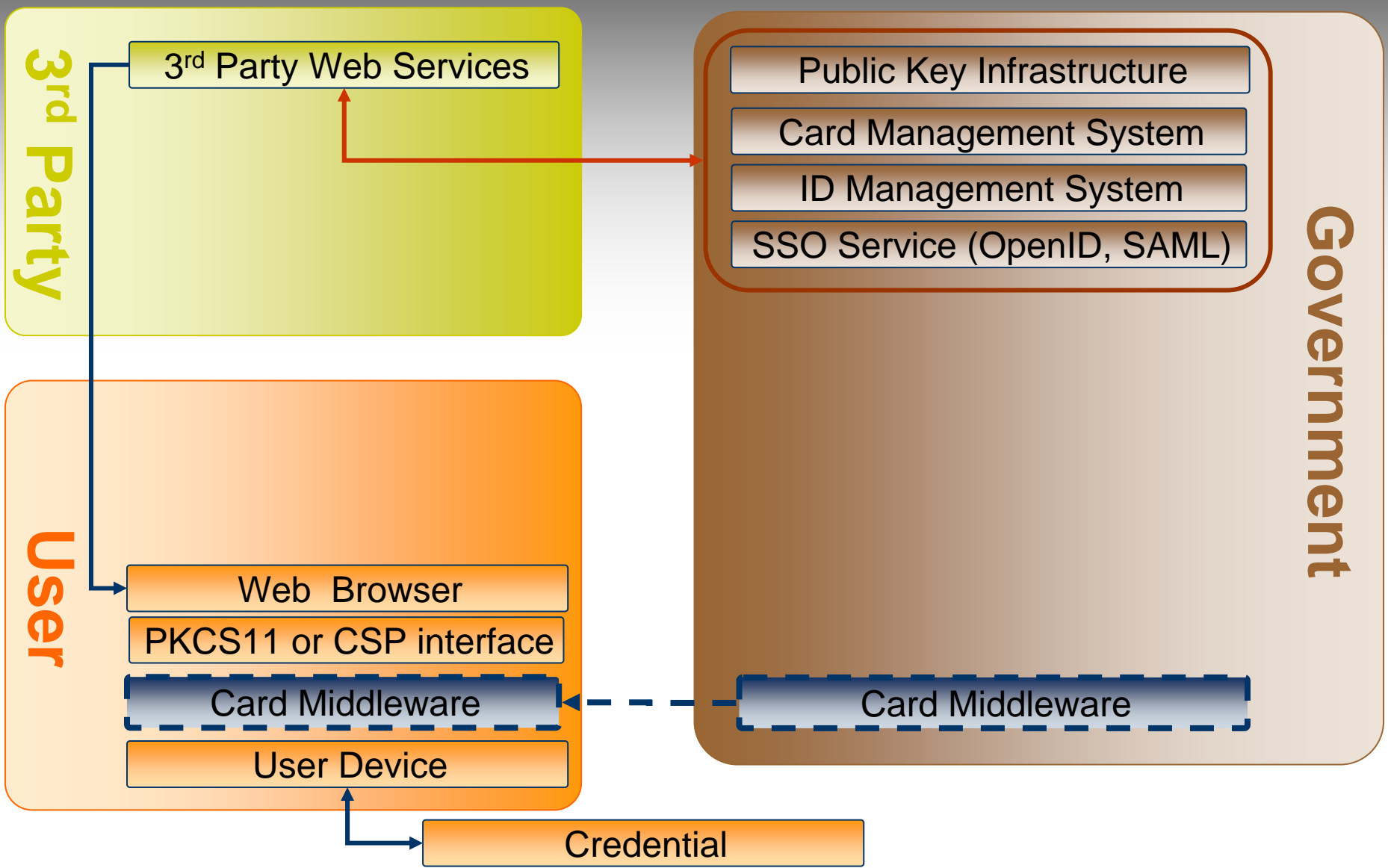
- Enrolment
 - How do I enroll accurate information?
- Issuance & Activation
 - How do I ensure the credential is provided to the right person and no one else uses it?
- Credential Management
 - How do I manage the card's life cycle?
- Credential Validation and Use
 - How do I ensure that services and users adopt this credential?
 - How do I provide support?

- Most common uses for Citizen credentials:
 - Form Filling
 - Authenticating
 - Signing
 - Ciphering

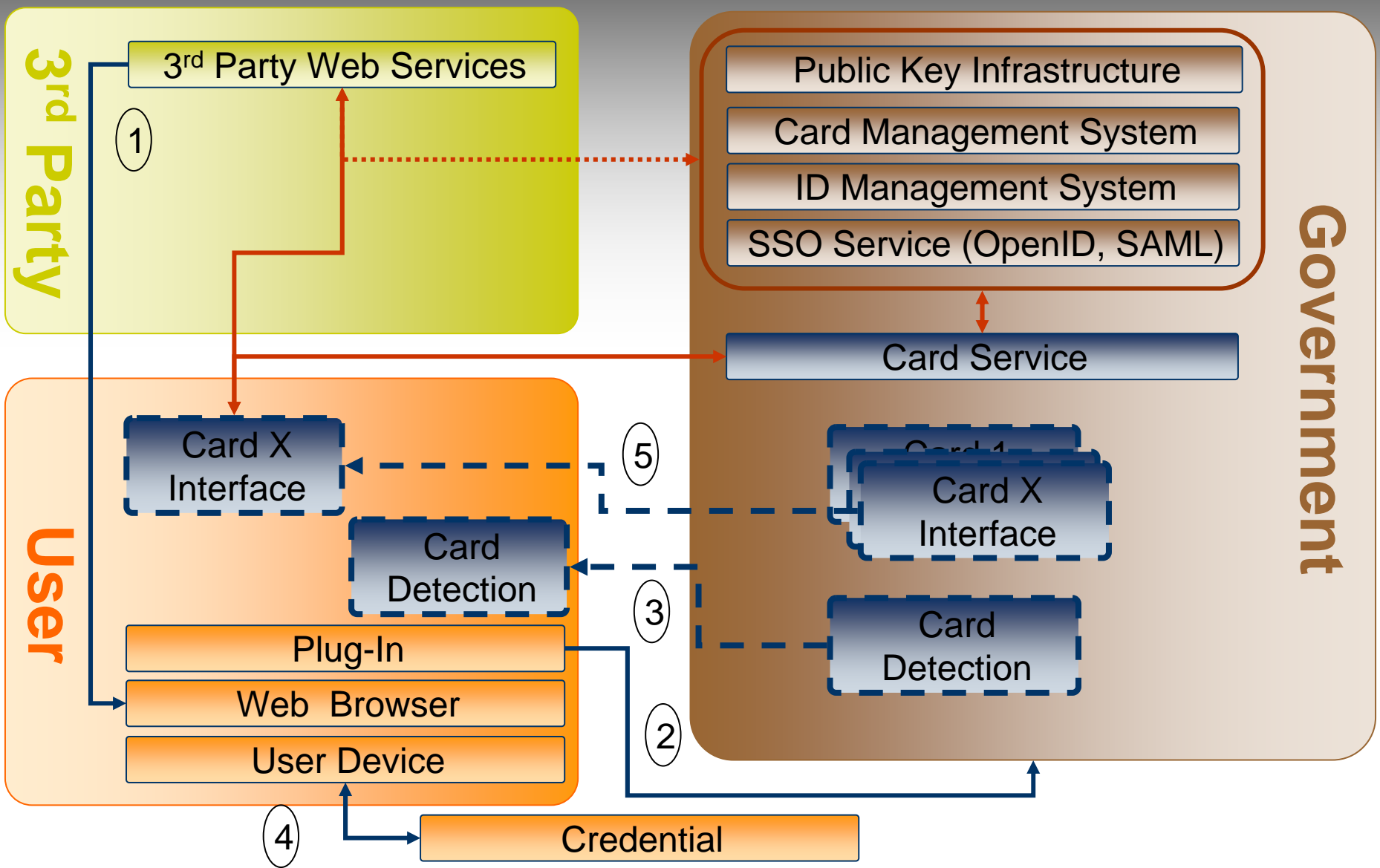
- Trends show all of these applications will soon be handled only through web applications.

- One obvious exception: Desktop login requires a domain and a CA and is usually reserved for the enterprise.

- Governments distributes a middleware composed of:
 - a CSP
 - a PKCS#11 library (on Windows, Linux and Mac)
- Middleware updates require that all users download and re-install the software.
- Support must be provided at the user level because of
 - Conflicting software or hardware
 - Middleware version issues
 - User access rights



- An authentication server
 - Provides the latest credential interfaces
 - Interfaces with PKI, CMS and IDMS
 - Can be used to provide services such as OpenID and SAML
- A minimalistic web browser plug-in that is installed as easily as the Flash Player.
 - Downloads the latest credential recognition information.
 - Recognizes the credential.
 - Downloads the credential specific interfaces.
- For smart cards this requires only a working PCSC stack on the user side.



- Low maintenance system
- Reduce distribution problems:
 - The latest middleware for the card being used is downloaded as needed by the browser.
- Reduce end user support problems:
 - Installs seamlessly as a browser plug-in (like Flash player for example).
 - Interaction with only the browser means less support calls due to the user's configuration.
- Reduce migration problems:
 - New cards are supported by all applications as soon as they are added to the central authentication server.

- Ultra fast learning curve for all parties involved
- Application support
 - Any web developer can easily integrate token usage in new or existing applications using a few lines of JavaScript.
 - Automatic support for all tokens supported by the server.
 - Use of AJAX allows the remote authentication service to automatically perform additional tasks like SSO.
- User adoption
 - Easy install means immediate use.
- Government deployment
 - Deploy right away as updates are easy!!!

- JavaScript interface
- Always up to date
- Built-in support for a number of existing cards including:
 - PIV-II End Point (NIST)
 - IAS ECC (European Citizen Card)
 - Muscle Applet (Open Source)
- Built-in support for biometrics and even OTP tokens
- An SDK to add new cards (about 1 week of work)
- Existing OpenID and SAML solutions

- **Try it now with Oberthur PIV, IAS ECC cards or load Muscle on an Oberthur ID-One Cosmo card:**
 - <http://openid.trustbearer.com>
 - <http://bank.trustbearer.com>
 - <http://apps.trustbearer.com/demo>