The Intel Identity Capable Platform

An Intel Research Project

Conor P. Cahill

Principal Engineer

Intel Corporation

Agenda

- Liberty ID-WSF Advanced Client Specifications
- Intel's ICP Research Platform
- Overview of Intel/BT/Symlabs Demonstration
- Vince will run the demo

Evolution of Liberty related Clients

- Phase 1: Liberty Enabled Client/Proxy (LECP)
- Phase 2: Active Client
- Phase 3: Advanced Client (aka Intelligent Client)
- Phase 4: Robust Client

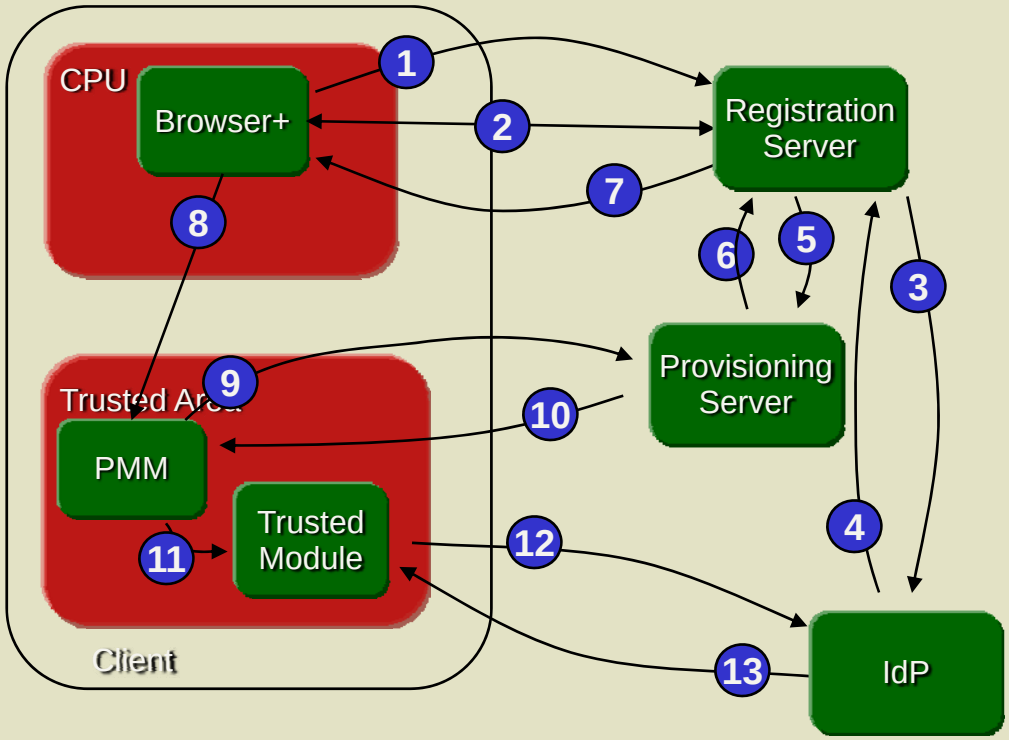
Advanced Client

- The client as an extension of a Service Provider
  - Identity Provider (IdP)
    - Off-line and privacy enabling modes
    - Strong local authentication
- Provisioning functionality and/or Data to Client
- Locally hosted/managed services
- Reporting

Advanced Client: Provisioning

- Functionality and/or data provisioning
- Full Lifecycle Management
  - Provision, Delete, Activate, Deactivate, Update
- Push and Pull (poll) options

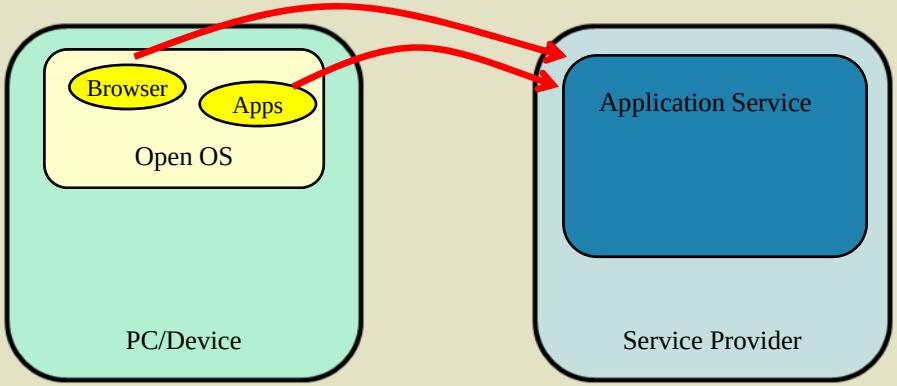
Provisioning A Trusted Module



1. User initiates registration through the browser
2. Registration Server (RS) collects information from the user
3. RS asks IdP for initial token
4. IdP generates token and returns to RS
5. RS creates Provisioning Descriptor (PMDesc) which includes initial token from IdP and registers PMDesc with Provisioning Server (ProvS)
6. ProvS generates Provisioning Handle (PH) and returns it to RS
7. RS sends PH to plug-in in browser
8. Browser plug-in sends PH to Provisioned Module Manager (PMM)
9. PMM decodes PH and invokes ProvS to get PMDesc
10. ProvS returns PMDesc to PMM
11. PMM Instantiates Trusted Module (TM) and passes in initialization data from PMDesc
12. TM generates private keys and registers them with IdP using initial token
13. IdP acknowledges registration

ICP Conceptual Overview

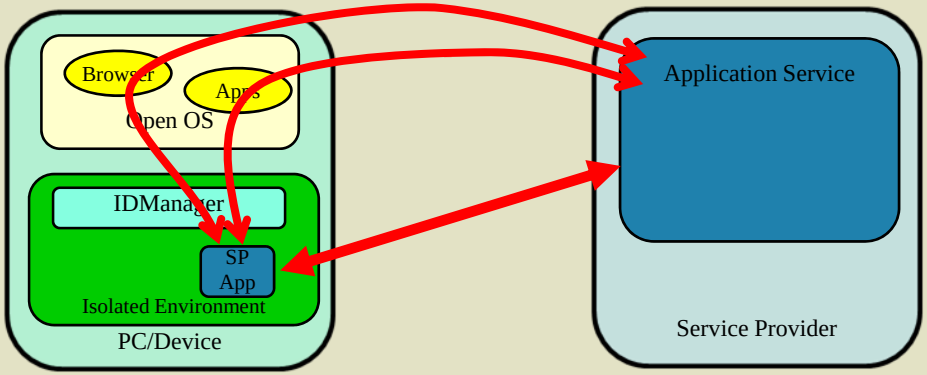
Today



Issues

1. Not secure
2. High risk
3. Limited functionality

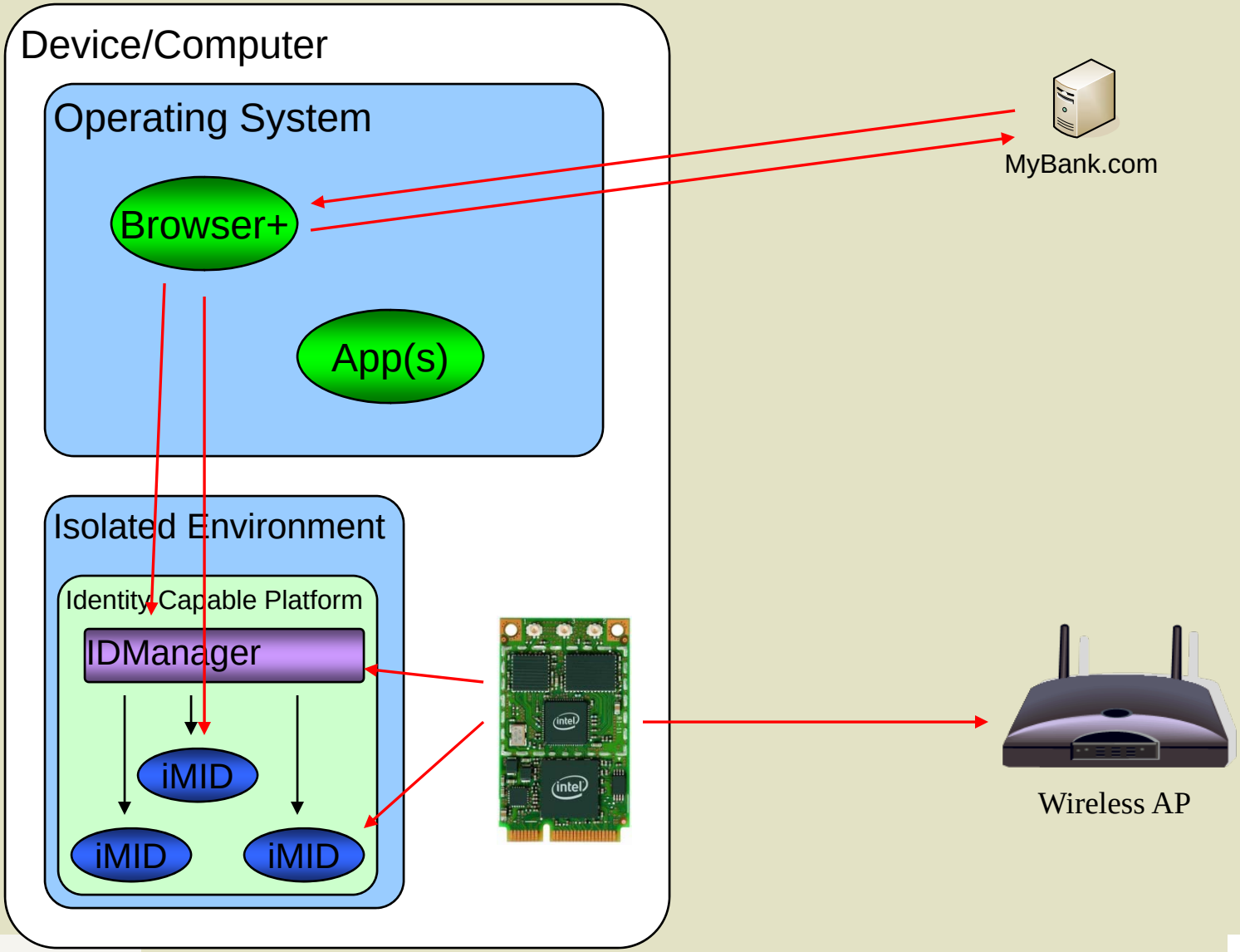
Tomorrow With ICP



Big Benefits

1. Highly secure
2. Much less risk
3. New capabilities

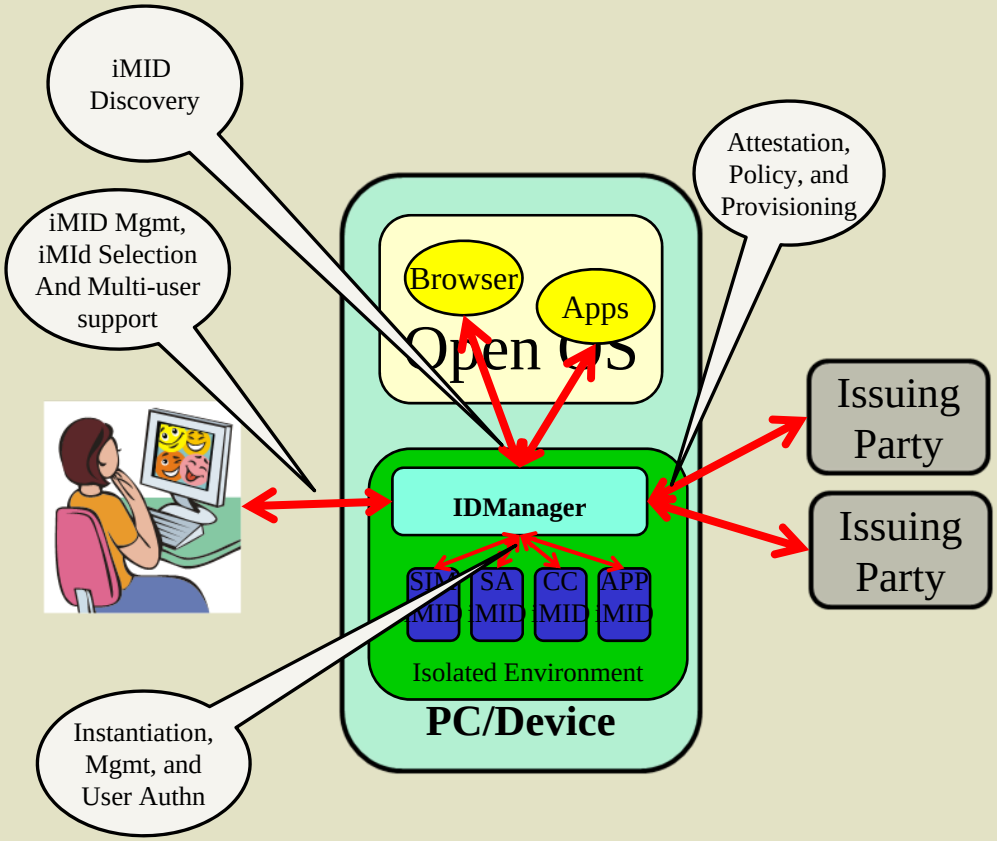
The Identity Capable Platform



The Identity Capable Platform

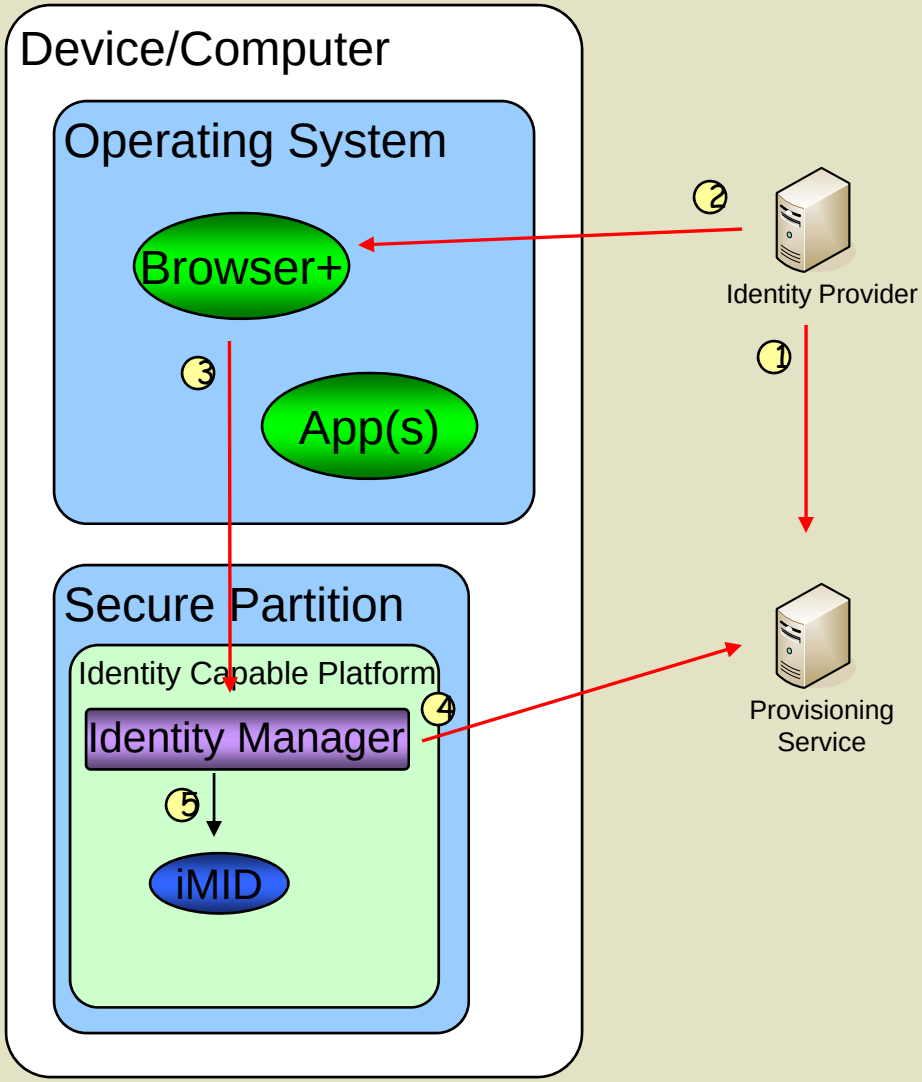
- A trusted environment
  - An Identity Manager (IDManager)
  - One or more Manageable Identities (iMID)
- Full lifecycle support for Manageable Identities
  - Provision, update, delete
  - Activate, deactivate
  - Serialize/deserialize
  - Portability
  - Over the wire/air as well as physical provisioning
- Policy controlled access and operations
  - Which user can access which iMID
  - What can be done with each iMID

IDManager Features/Capabilities



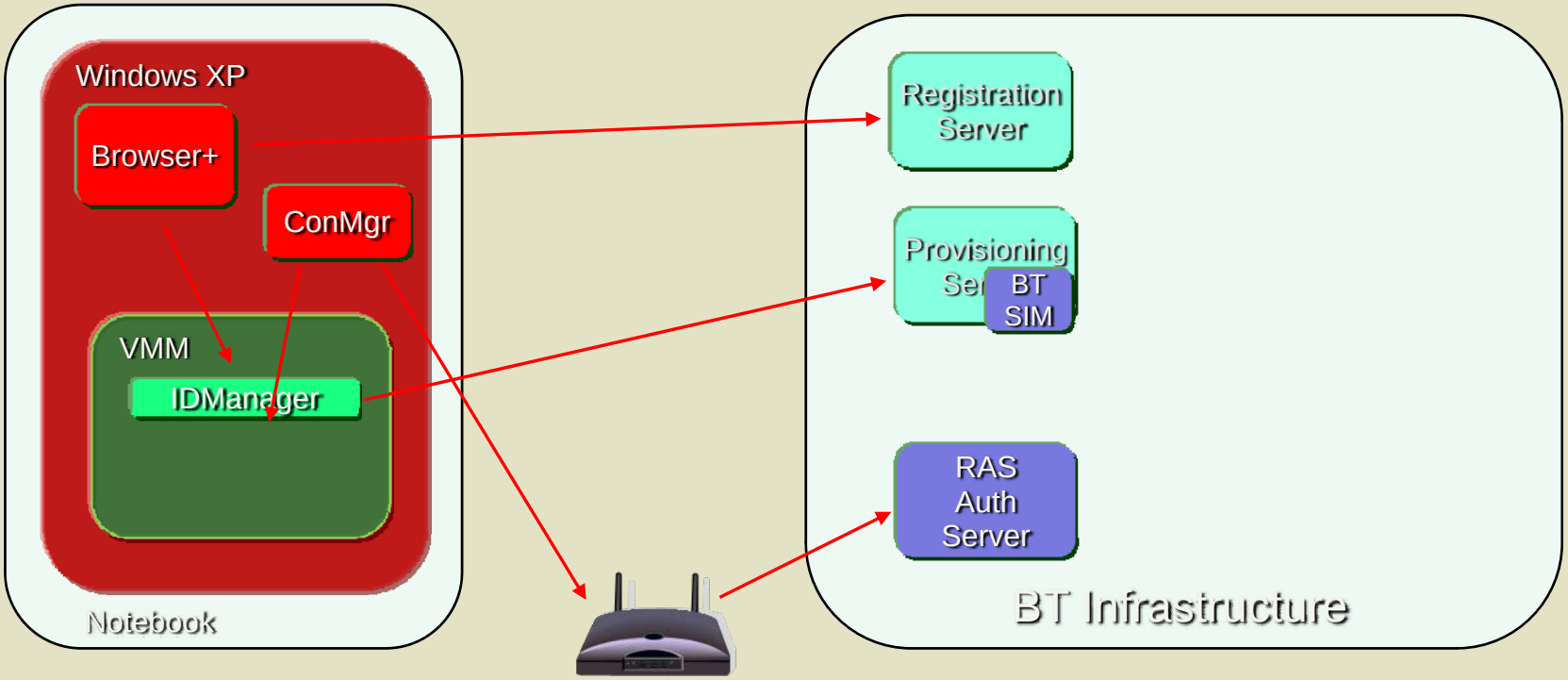
- Issuing Parties
  - Platform Attestation
  - iMID Policy Enforcment
  - Provisioning & Lifecycle management
- Browsers/Apps
  - iMID Discovery
- iMIDs
  - Instantiation
  - Management Interfaces
  - User Authentication
- Users
  - iMID Management (list, remove, stop, restart)
  - iMID Selection
  - Multi-user support

Provisioning an Identity in the ICP

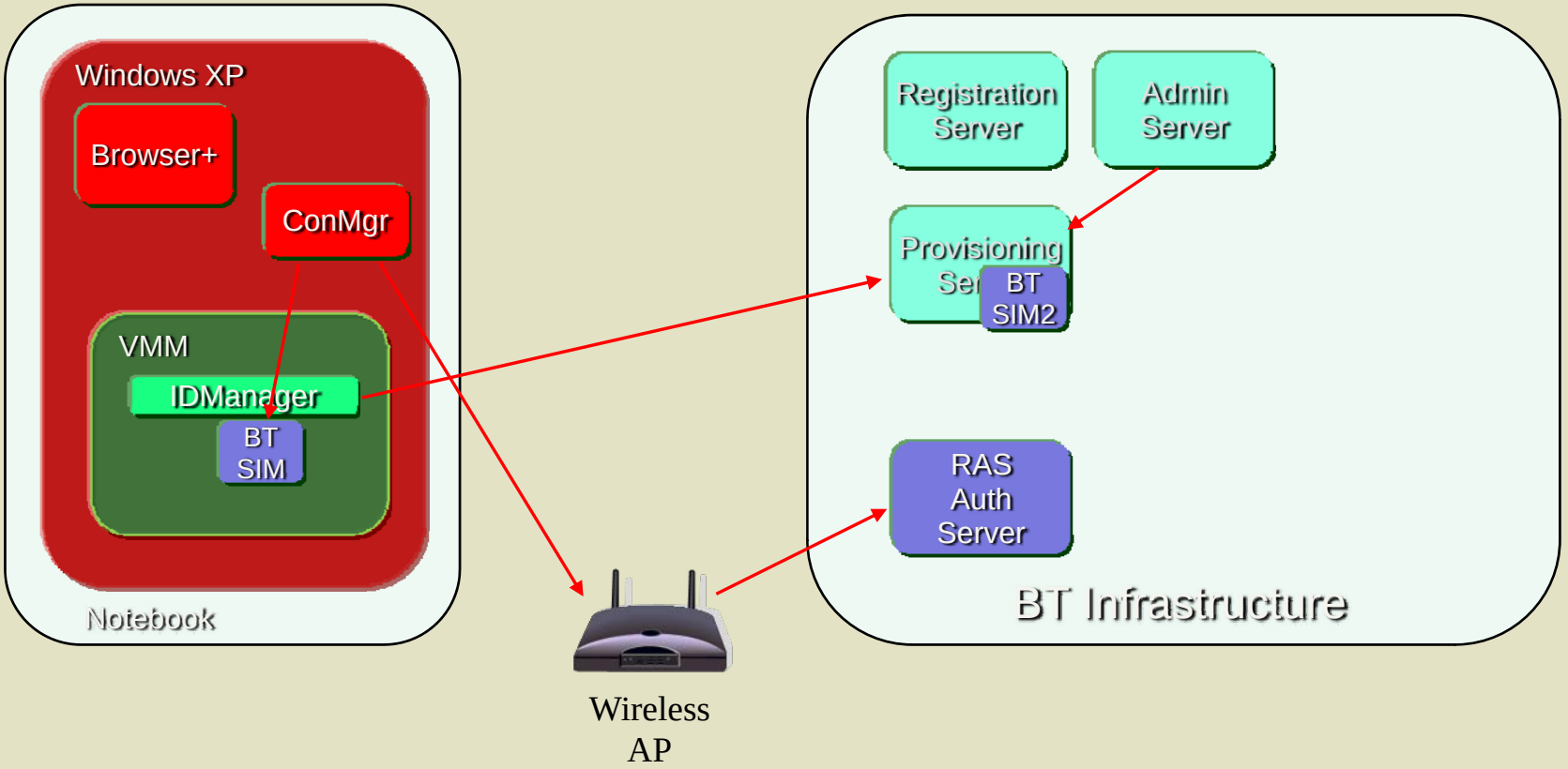


1. The Identity Provider registers the Identity to be provisioned at the Provisioning Service
2. The Identity Provider sends a reference to the identity to the browser with instructions to send the reference to the Identity Manager.
3. The browser submits the identity reference to the Identity manager
4. The Identity manager dereferences the identity at the Provisioning service and gets back the Identity
5. The Identity Manager instantiates the Identity within the ICP.

Intel/BT/Symlabs Demo: Provision



Intel/BT/Symlabs Demo: Update



More Information

- Web
  - http://www.intel.com/technology/systems/stl/
  - http://www.projectliberty.org
  - http://www.symlabs.com
- Email
  - Conor Cahill - ICP Principal Engineer
    - Conor.P.Cahill – at – Intel.com