



Tivoli Security Products

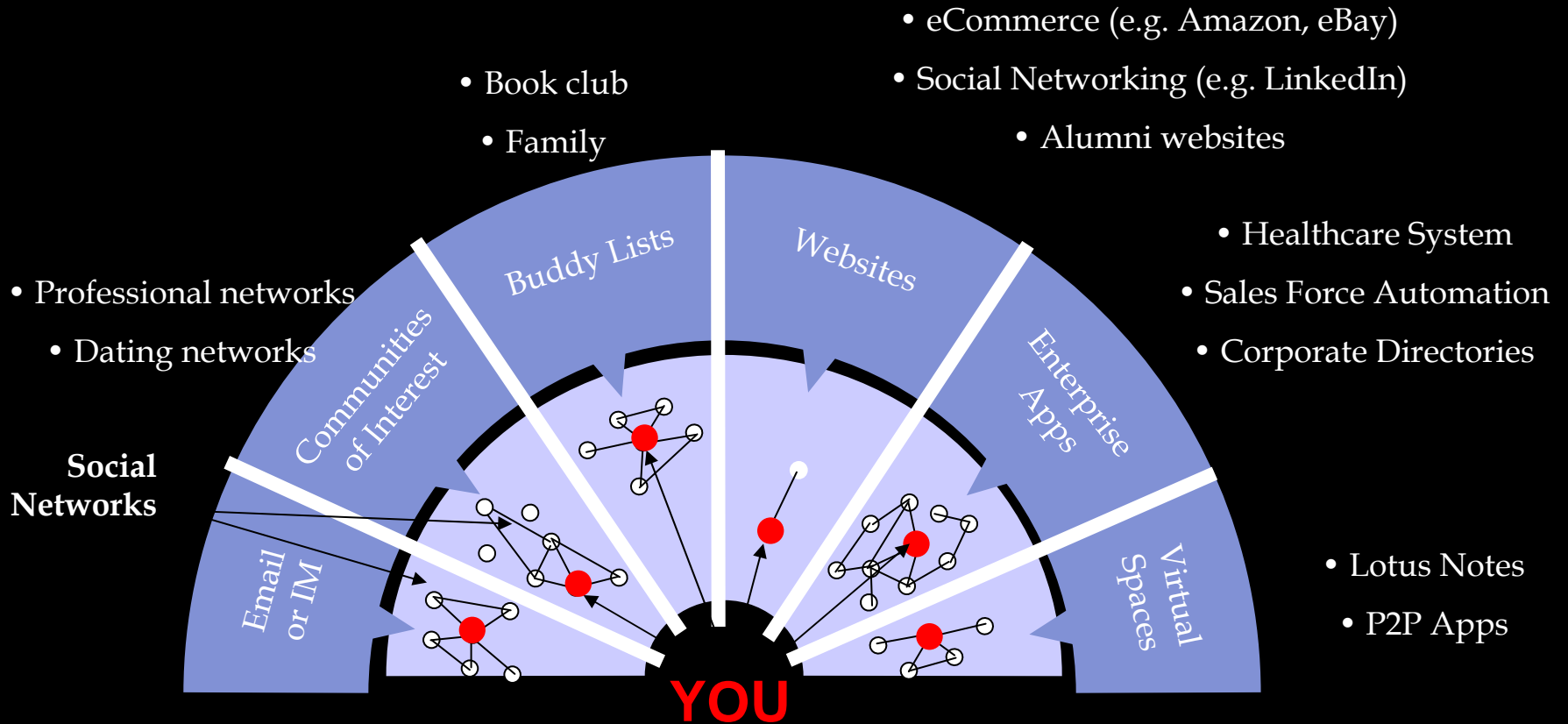
Higgins Fly-By

Bruce Rich
Security Architecture and Standards

5/14/2009

© 2009 IBM Corporation

Siloed Identity



Higgins



- 1) A species of Tasmanian long-tailed mouse
- 2) An open-source identity framework developed at the Eclipse foundation

Goals

- **Identity framework for Internet-enabled applications**
- **User in control of what gets shared**
 - Selector, card-based interaction
- **Identity integration**
- **Platform/OS agnostic**
- **Extensible architecture**
- **Open-source, community-based project**

Identity Ecosystem

- **Cards**
 - View of my identity
 - User chooses which card
- **Producers and consumers**
 - Cards and runtime representations
- **Identity mines**
 - Identity attribute service

Cards, Selectors, Choices

Any tidbit of information
(home address, birthdate,
camera preference) might
comprise a portable claim
to be put on a card



Cards from different
providers are managed
in an Identity Selector

Pick a card, any card



I create (personal)

- I define a few personas
- Business “me”, web surfing “me”, dating “me”



Others create (managed)

- Credit cards
- Membership, reputation in community
- 3D avatar (virtual identity)
- Governments (drivers license)



I co-create with others (relationship)

- My preferences, interests within community
- Might include shopping history and wishlists

Identity Services



- Identity Providers (IdP) vouch for the identity claims (produce a runtime token)
- Relying Parties (RP) look for identity information from Identity Providers they trust

Identity Providers

- WS-Trust IdP/Security Token Service
 - Web service
 - Card issuer
- SAML2 IdP
 - Web service

Attribute Services



Web services and other building blocks related to accessing identity attributes

Identity Attribute Service, Context Data Model,
RDF/OWL

Additional information

- **Higgins website** = <http://www.eclipse.org/higgins>
- **Dig deeper** = <https://dev.eclipse.org/svnroot/technology/org.eclipse.higgins/trunk/doc/org.eclipse.higgins.doc/Higgins-Overview-2009.pdf>
- **OASIS Identity Metasystem Interoperability TC** = http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=imi

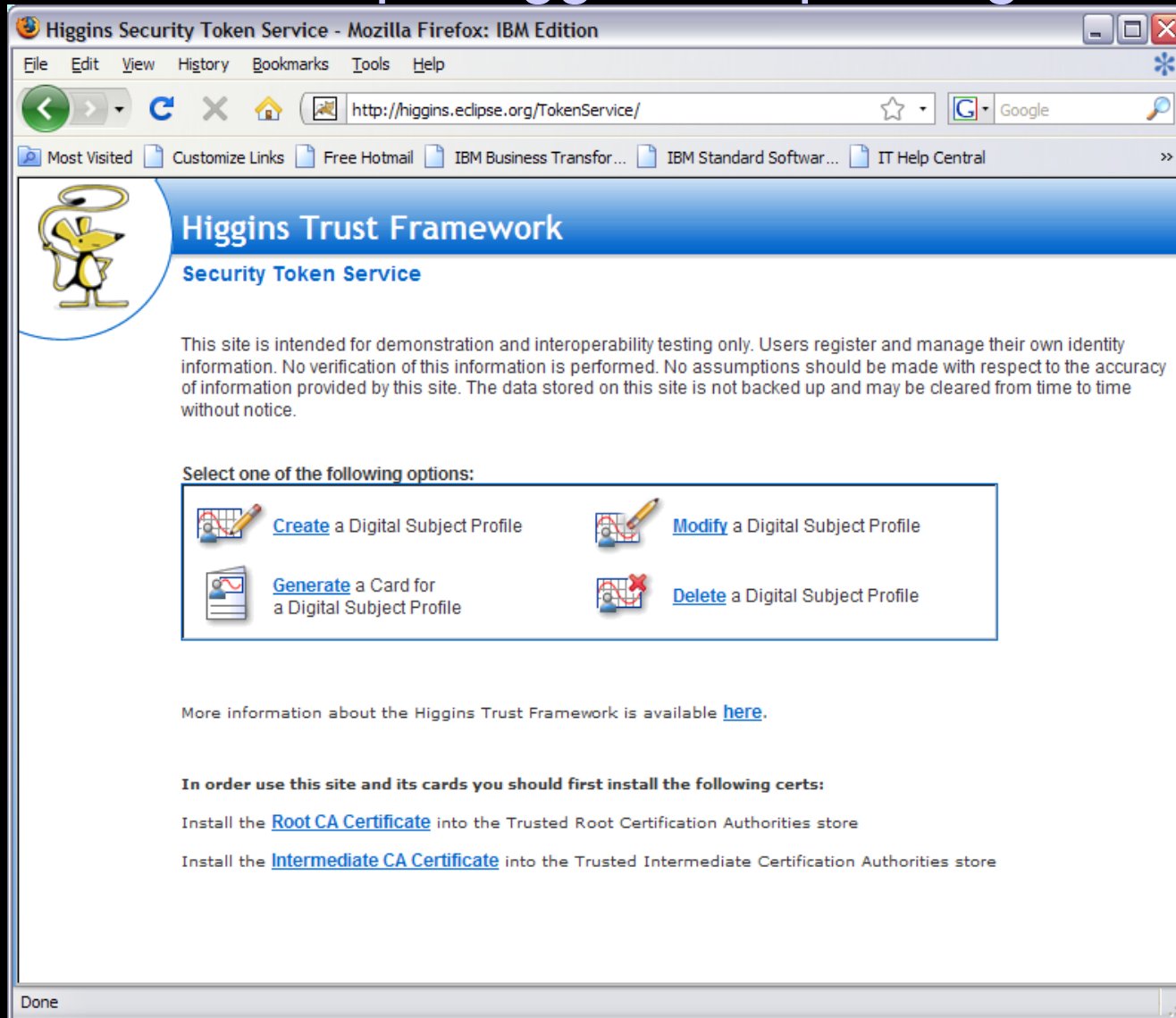


BACKUP MATERIALS

Card vs Cookie – what's the diff?

- Card = user-centric (not machine)
- Card = context-sensitive and under user control
- Card = cryptographically-difficult to attack

WS-Trust IdP @ <http://higgins.eclipse.org>



Higgins Security Token Service - Mozilla Firefox: IBM Edition

File Edit View History Bookmarks Tools Help

[http://higgins.eclipse.org/TokenService/](#) Google





Most Visited Customize Links Free Hotmail IBM Business Transfor... IBM Standard Softwar... IT Help Central

Higgins Trust Framework

Security Token Service

This site is intended for demonstration and interoperability testing only. Users register and manage their own identity information. No verification of this information is performed. No assumptions should be made with respect to the accuracy of information provided by this site. The data stored on this site is not backed up and may be cleared from time to time without notice.

Select one of the following options:

 Create a Digital Subject Profile	 Modify a Digital Subject Profile
 Generate a Card for a Digital Subject Profile	 Delete a Digital Subject Profile

More information about the Higgins Trust Framework is available [here](#).

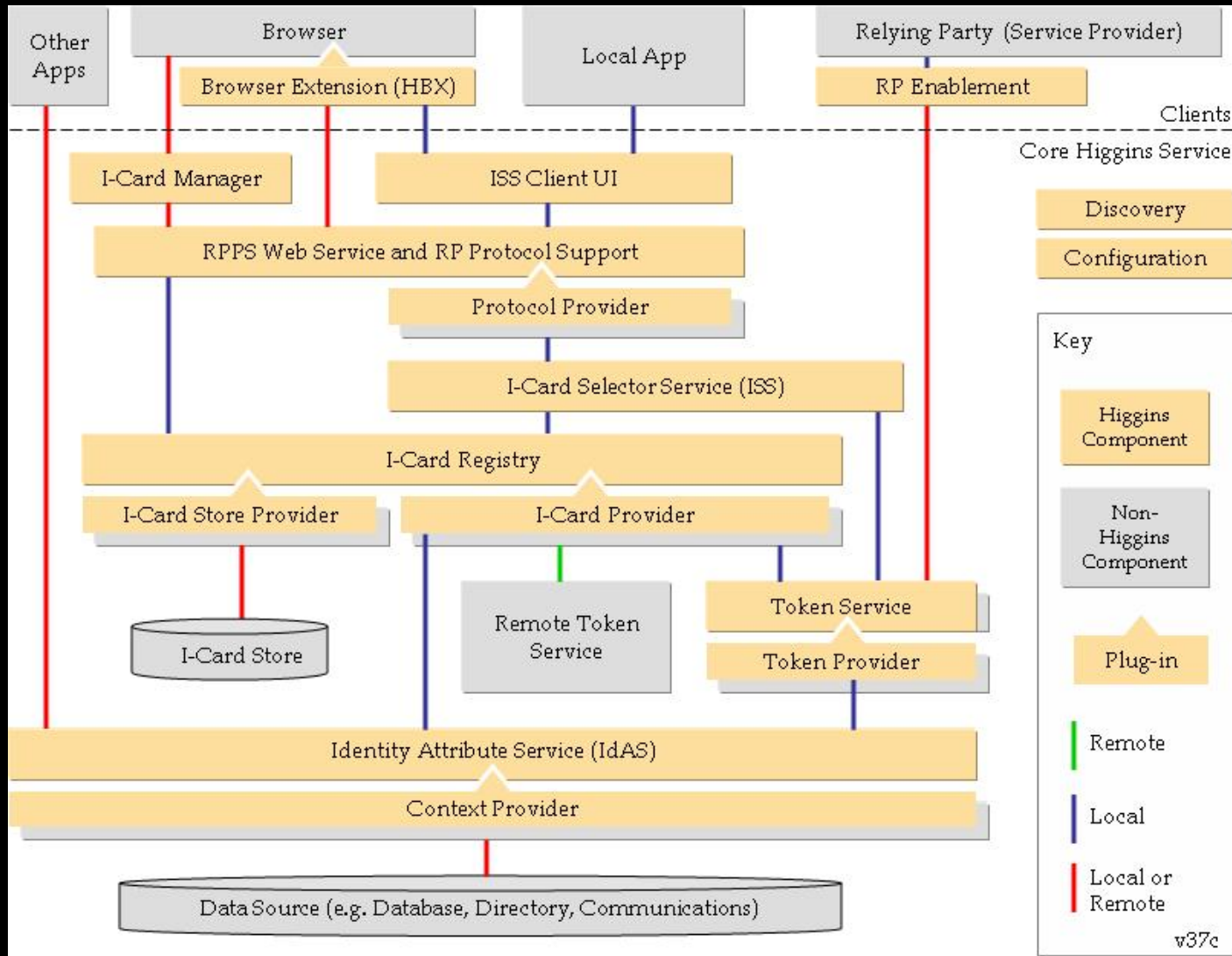
In order use this site and its cards you should first install the following certs:

Install the [Root CA Certificate](#) into the Trusted Root Certification Authorities store

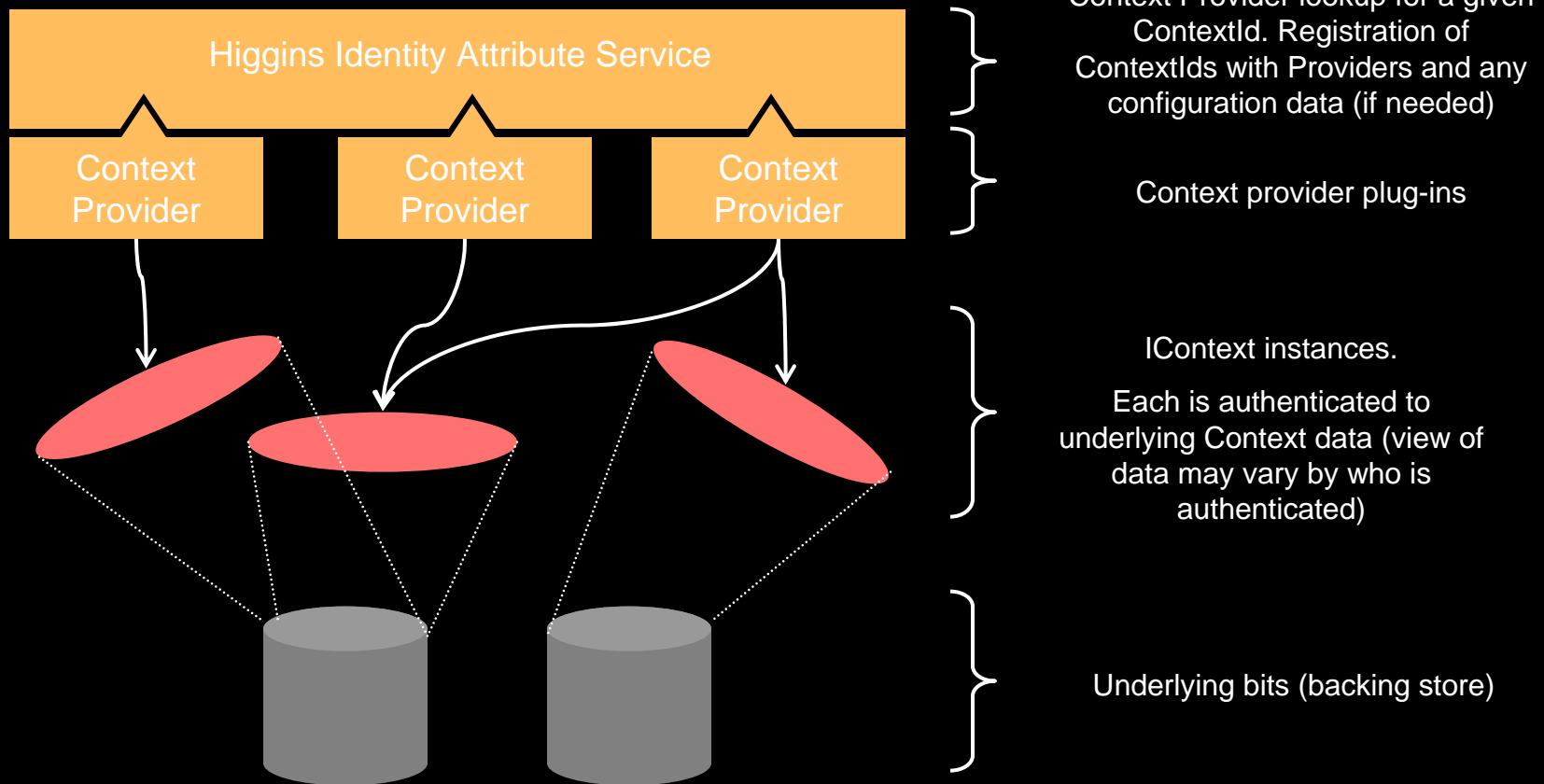
Install the [Intermediate CA Certificate](#) into the Trusted Intermediate Certification Authorities store

Done

Higgins Architecture



Context Providers: Mapping data into the Higgins model



Anticipated Higgins 1.1 content

- Selector-selector – can choose which selector gets called
- AIR-based selector
- Relationship card + password card
- iPhone selector
- Web selector (OpenID)
- Google Contacts context provider
- ...