

Microsoft® Research

Faculty Summit 2010

Delivering End to End Trust

Jeffrey Friedberg

Chief Trust Architect
Microsoft Corporation

Trustworthy Computing



Security

- Secure against attacks
- Protects confidentiality, integrity and availability of data and systems
- Manageable



Privacy

- Protects from unwanted communication
- Controls for informational privacy
- Products, online services adhere to fair information principles



Reliability

- Dependable, Available
- Predictable, consistent, responsive service
- Maintainable
- Resilient, works despite changes
- Recoverable, easily restored
- Proven, ready



Business Practices

- Commitment to customer-centric Interoperability
- Technology Accessibility
- Recognized industry leader, world-class partner
- Open, transparent

Path to End to End Trust

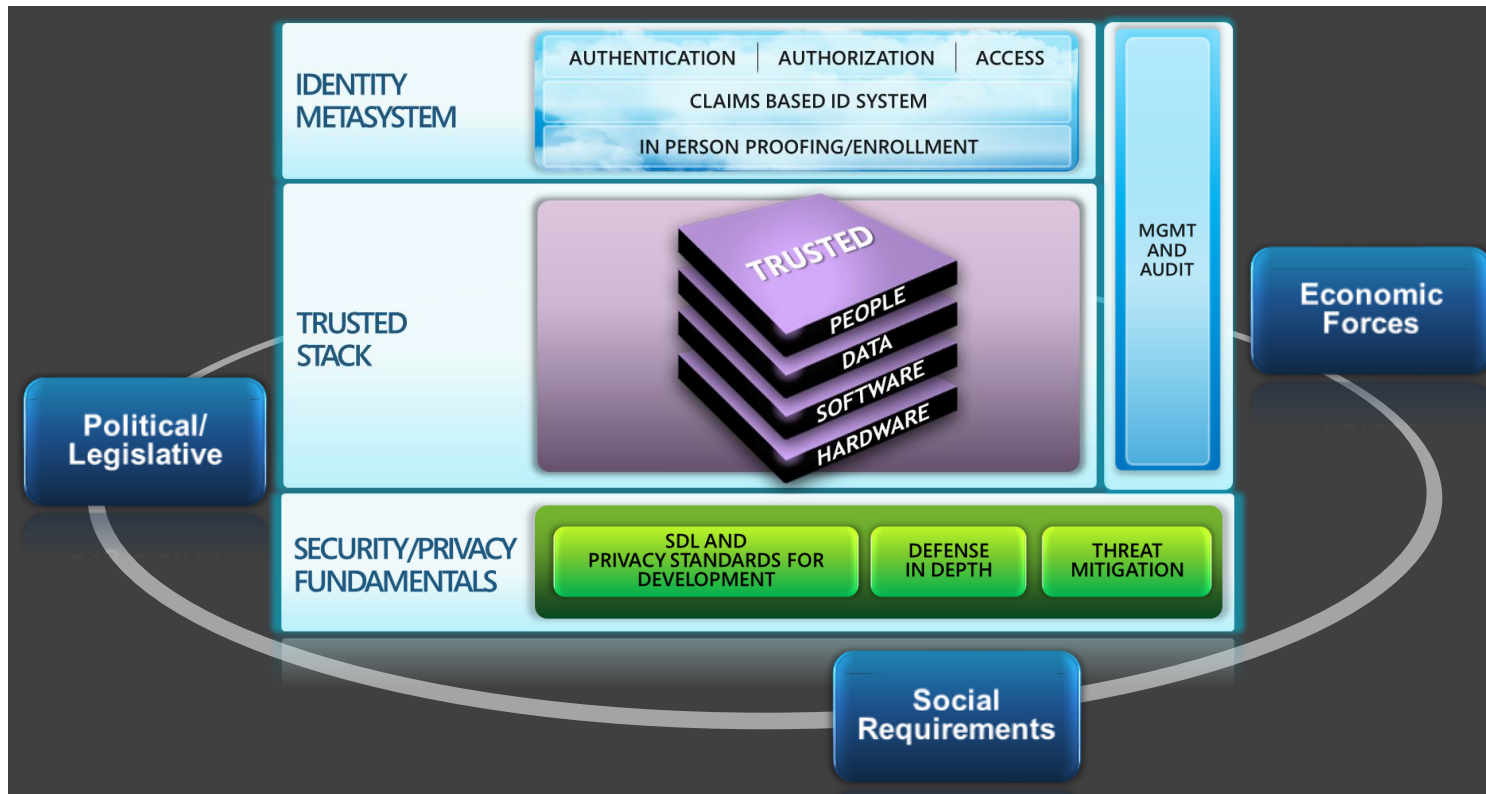
- 2002: Security Development Lifecycle
- 2005: Privacy Standard and Process
- 2006: Internet Battlefield, Identity Theft Analysis
- 2007: Trust User Experience (TUX) Team
- 2008: E2E Trust White Paper
- 2008: E2E Trust Team
- 2009: E2E Trust Roadmaps

End to End Trust White Paper

- Many believe need better security, privacy
- Greater connectivity and valuable targets lead to new threats and greater cybercrime
- Criminals anonymous and untraceable

- Need greater accountability
- Need to know who is who
- Need to have a trust framework

End to End Trust White Paper



- Conceptual vs. operational
- Who does what when?
- Apply standard PM techniques
- Create a roadmap

Roadmap Goals

- Help stakeholders see the “big picture”
 - Demystify, make it easy to see their piece
 - Analyze dependencies, critical paths
 - Highlight long poles like new standards, laws
 - Spot common building blocks across initiatives
 - Collaborate on implementation strategy
- Make insightful “calls to action”
 - Inspire and enable
- Track progress
 - Map activity, show trajectory

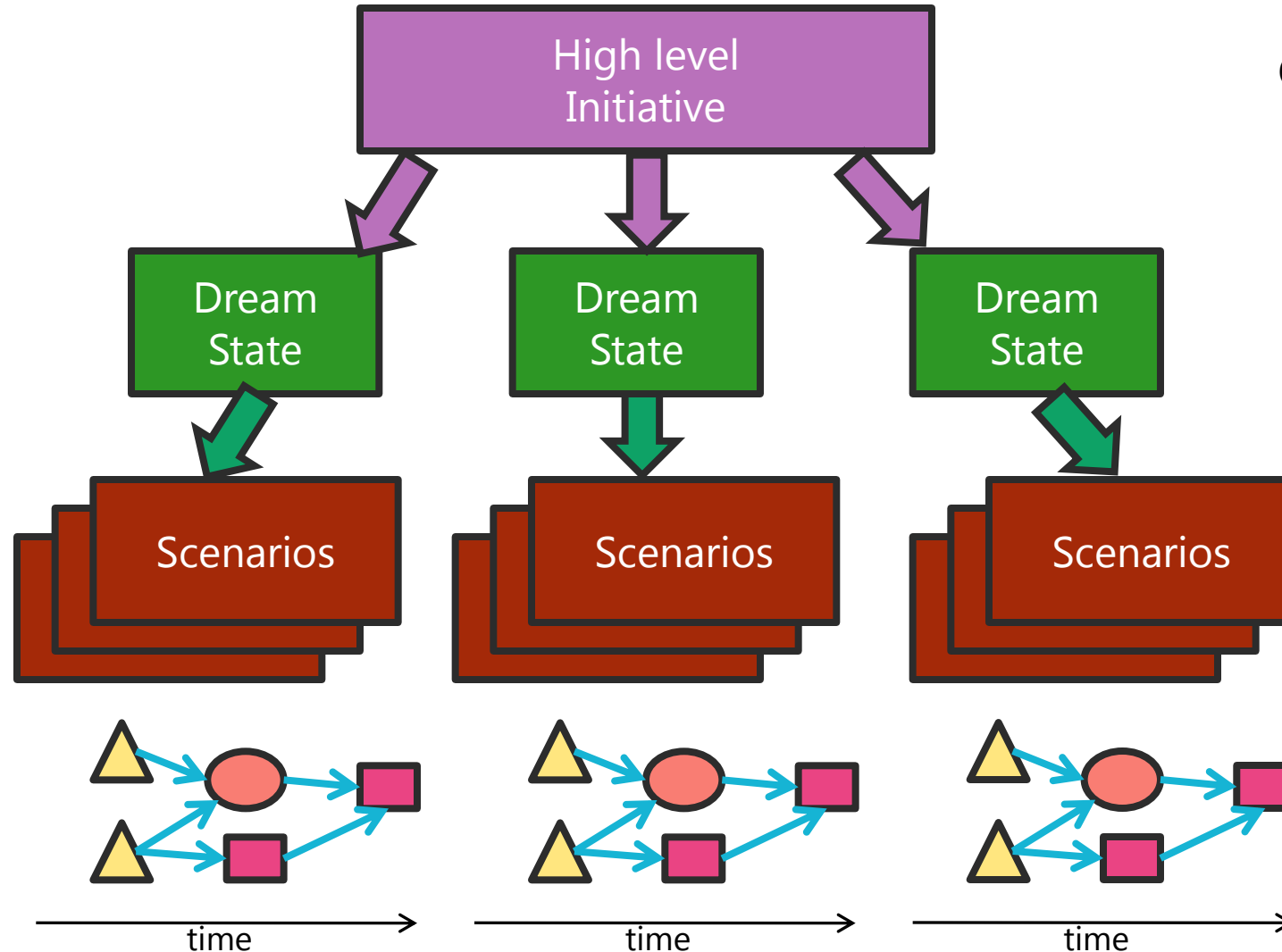
Roadmap Methodology

Start with a big play that has big impact for ecosystem

Identify high level wish list by stakeholder

Craft scenarios that embody the vision

Layout key building blocks by owner over time with dependencies



Online Health Care ...

Patient, provider, payer, regulator, researcher ...

Mary is traveling, feels sick ...

In person proofing, safe harbor, audit data standards ...

"SPICIER" Scenarios

- Tell a **STORY**
- **PERSONAL** details
- **IMPLEMENTATION FREE**
- **CUSTOMER** voice
- Deep **INSIGHT**
- User **EMOTIONS** and **ENVIRONMENT**
- Real **RESEARCH**

Example: Remote Care

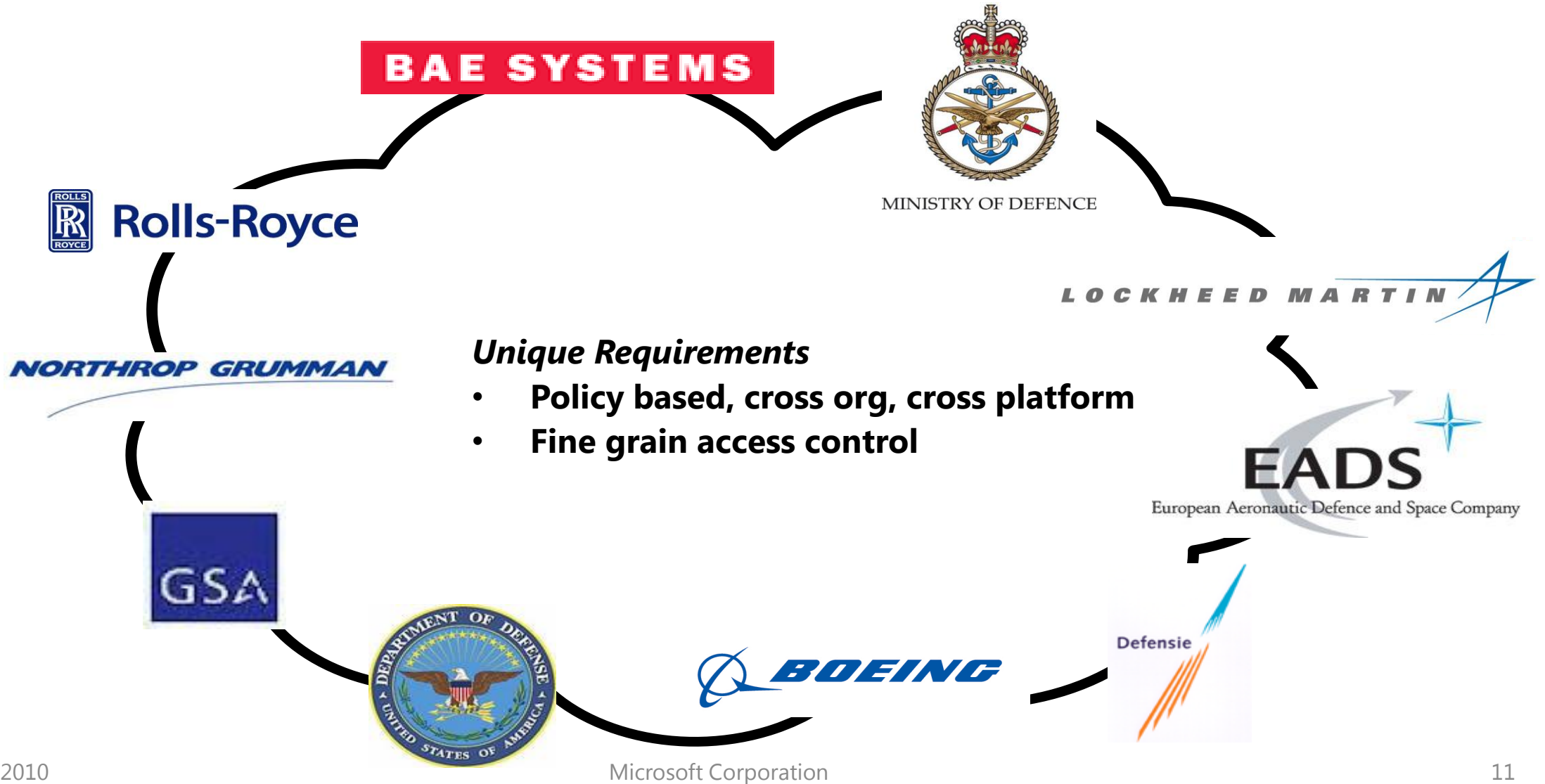


- Annie from Ontario is visiting her aunt in Saskatoon for the first time
- She develops throat pain and difficulty swallowing
- She is relieved to find a local walk-in clinic but they have no records for her
- Annie gives the doctor permission to see her online records just for this visit
- The doctor is able to access her records from his own computer
- Based on her history and allergies, the doctor confidently prescribes an appropriate medication
- Annie stops by the pharmacy, takes the medication, and starts feeling better

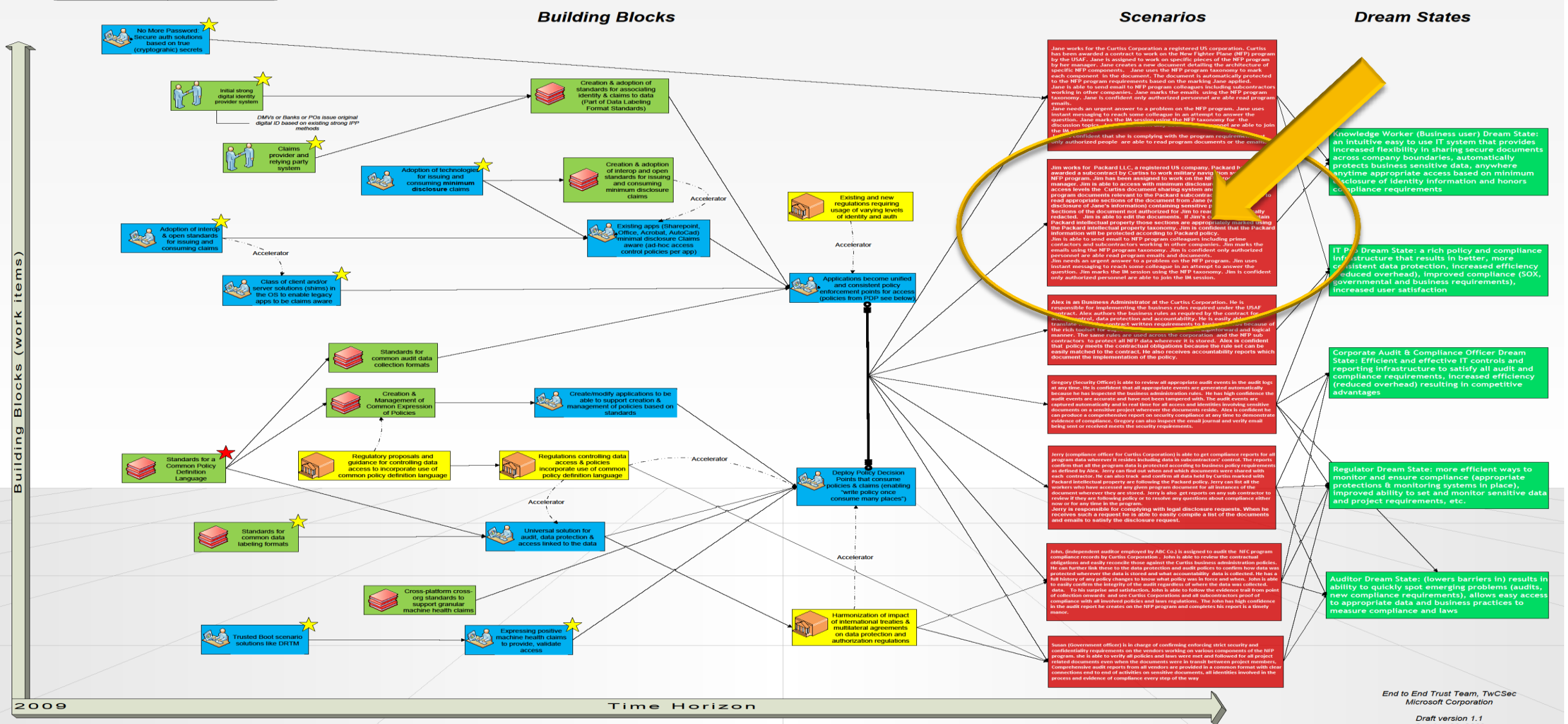
Key Initiatives

- Enable online health care
 - Manage privacy risks
- Enable eCommerce
 - Reduce online fraud
- Protect critical infrastructure
 - Preserve personal freedoms
- Enable secure online collaboration
 - Manage distrust between parties

Trans-global Secure Collaboration Program (TSCP)



Secure Collaboration

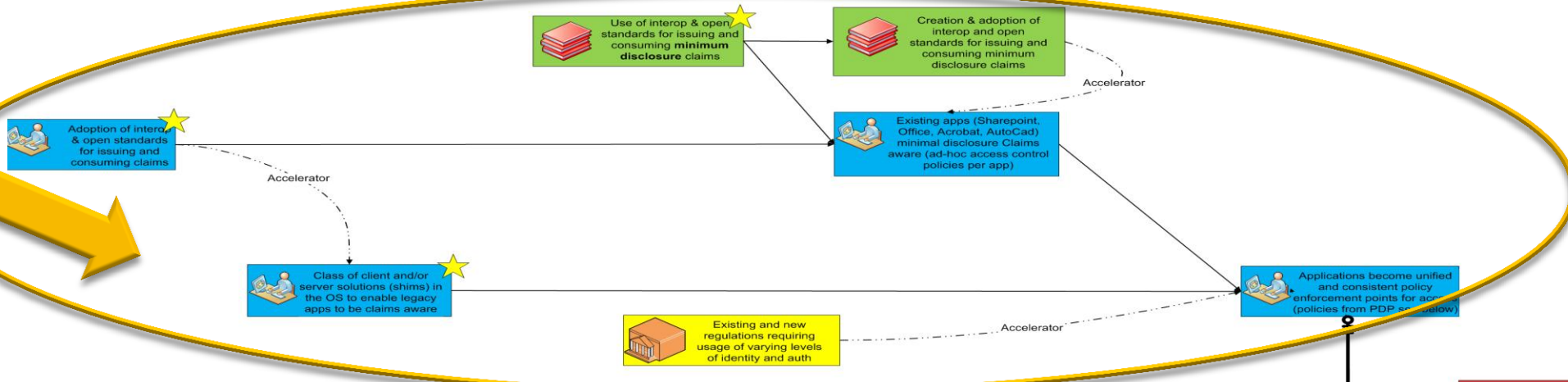


Scenario Simplified

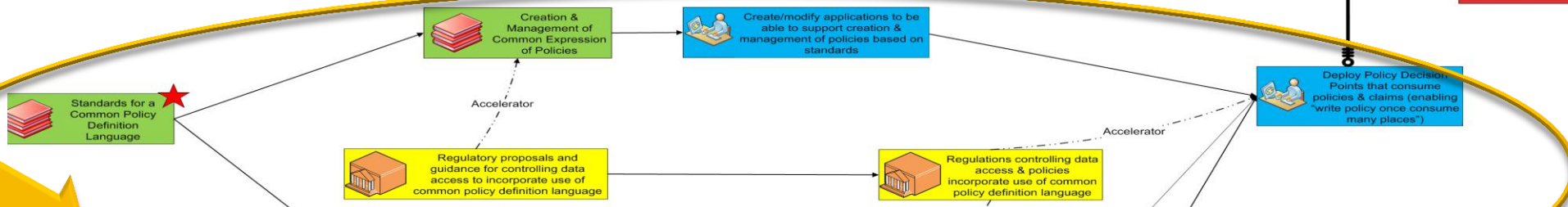
- Jim is able to securely collaborate and share sensitive project data
- With partners in multiple organizations
- Based on a common project taxonomy
- Regardless of the application being used

Building Blocks for Scenario

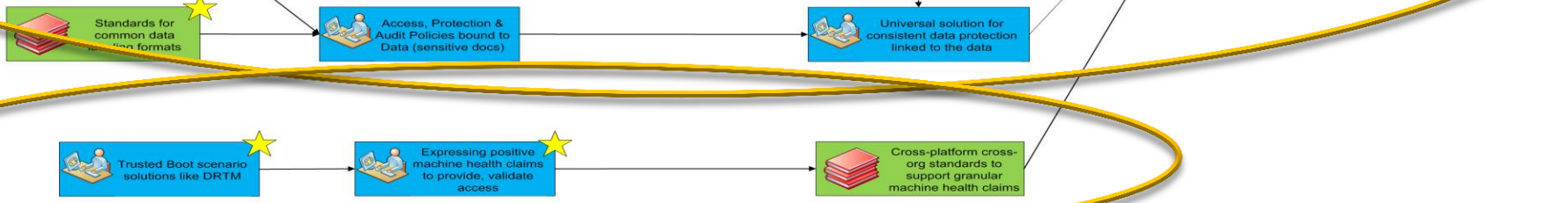
Identity Claims



Universal Policy Based Access

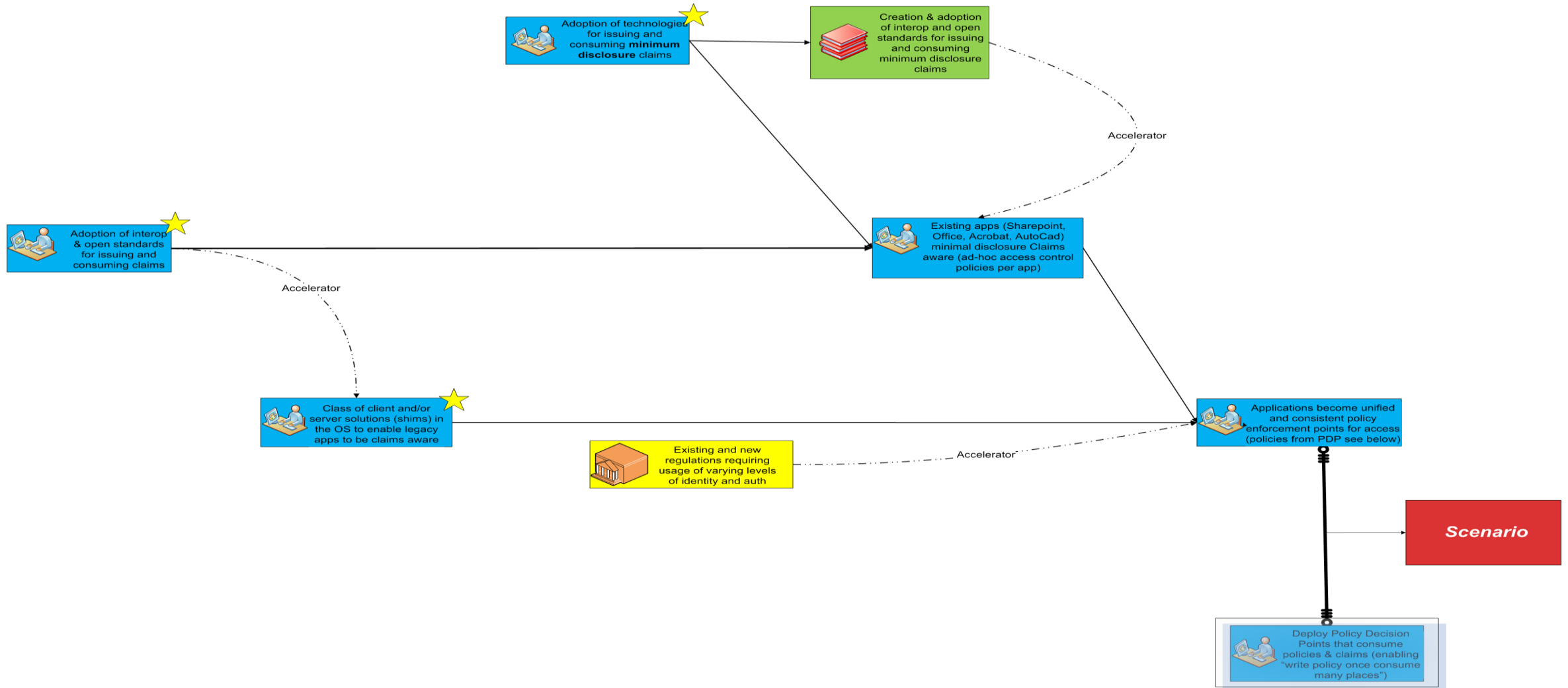


Machine Health Claims

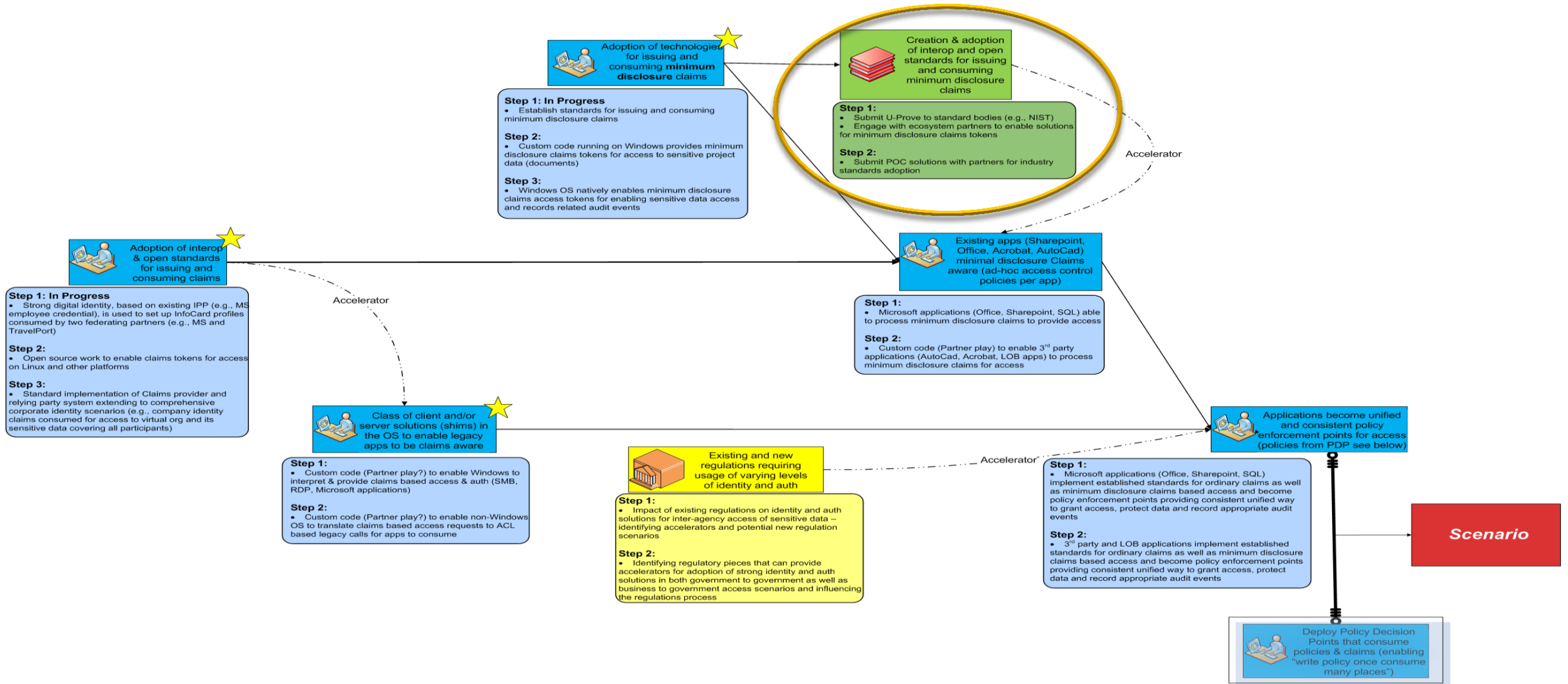


Scenario

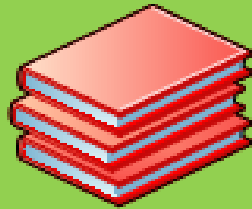
Identity Claims: Building Blocks



Identity Claims: Projects



Identity Claims: Standards Example



Creation & adoption
of interop and open
standards for issuing
and consuming
minimum disclosure
claims

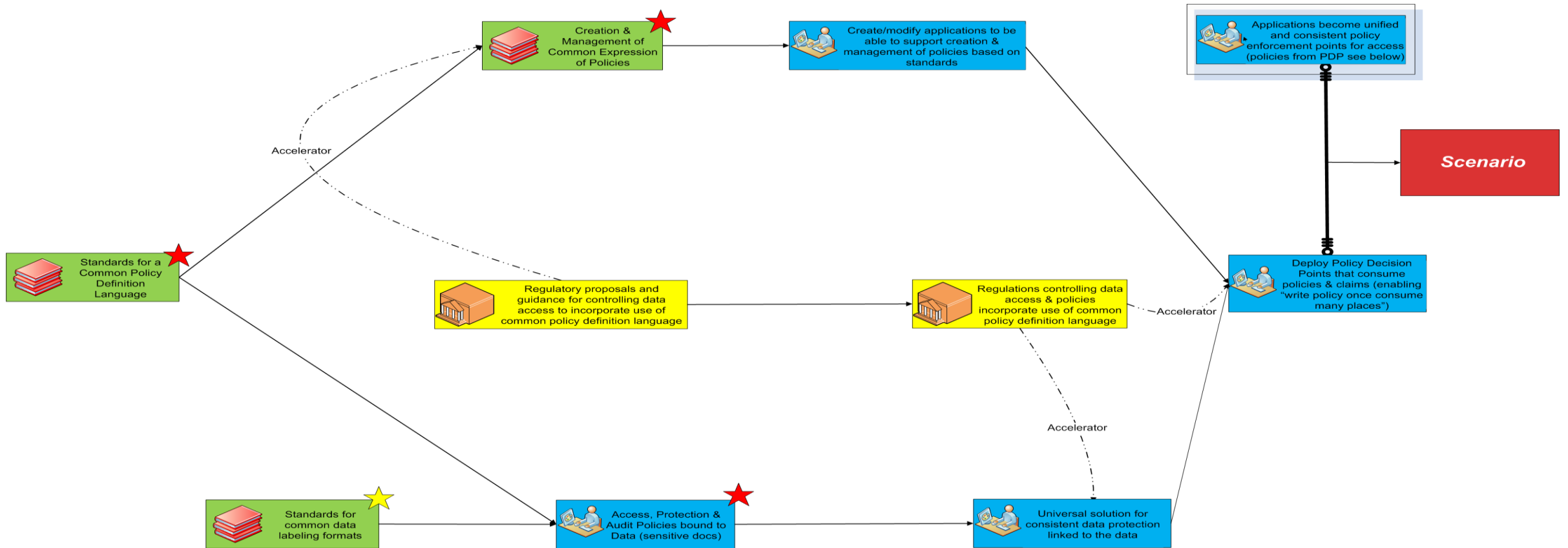
Step 1:

- Submit U-Prove to standard bodies (e.g., NIST)
- Engage with ecosystem partners to enable solutions for minimum disclosure claims tokens

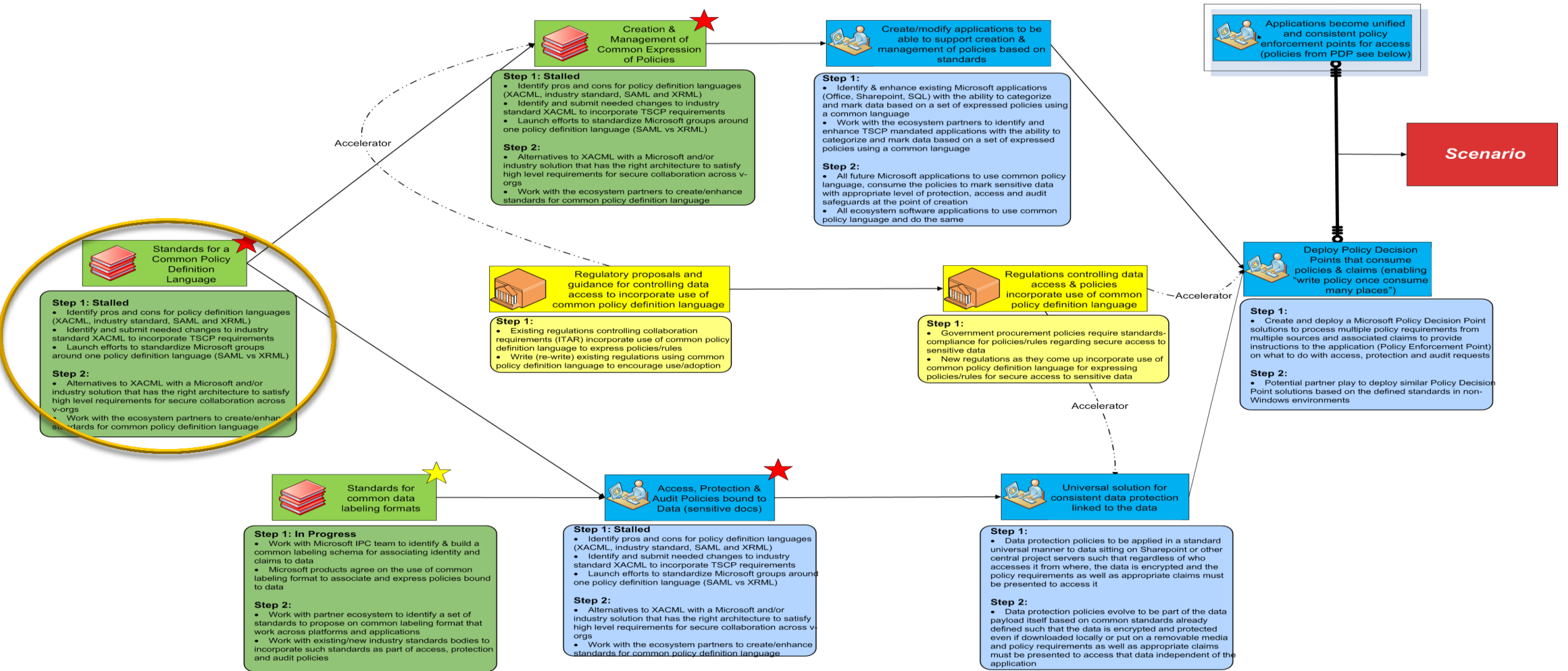
Step 2:

- Submit POC solutions with partners for industry standards adoption

Universal Policy: Building Blocks



Universal Policy: Projects



Universal Policy: Standards Challenge



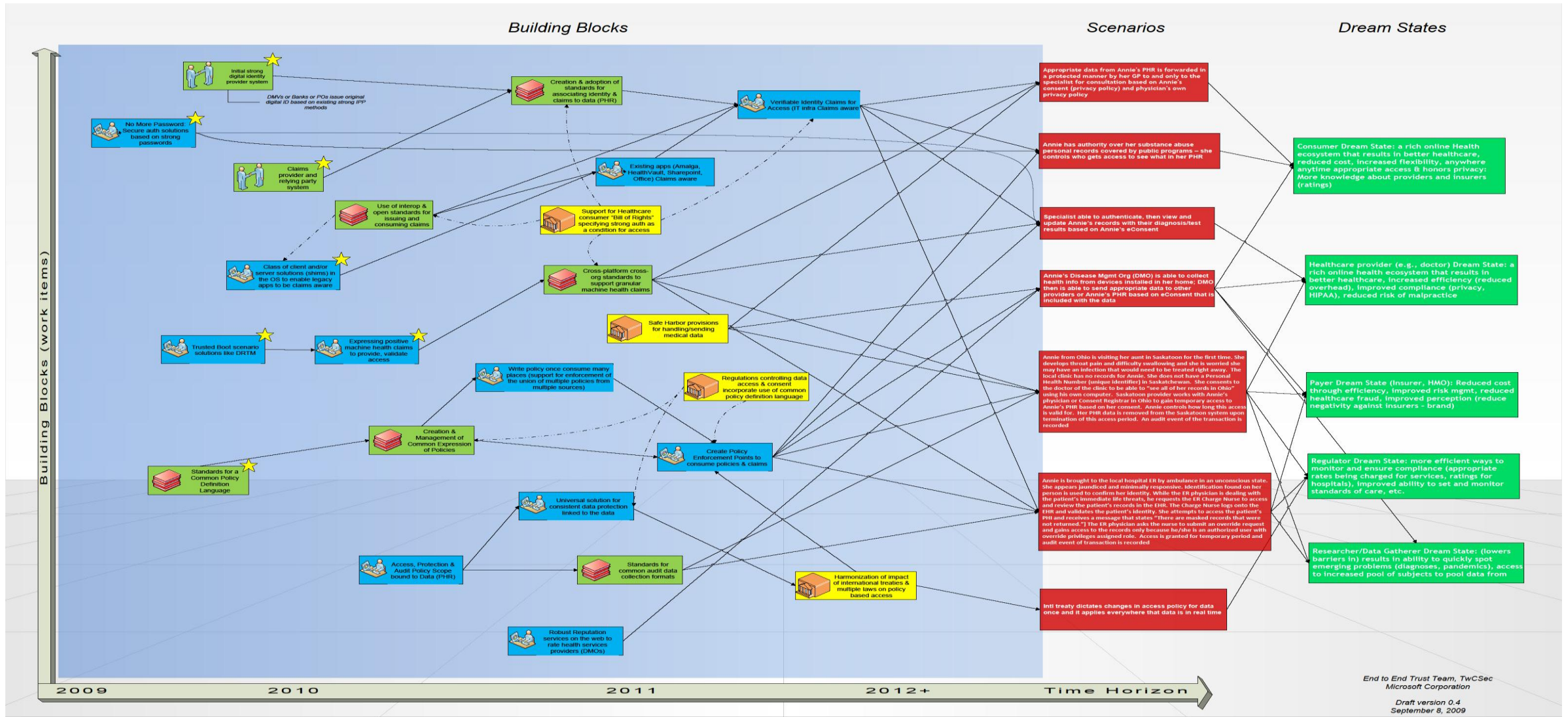
Step 1: Stalled

- Identify pros and cons for policy definition languages (XACML, industry standard, SAML and XRML)
- Identify and submit needed changes to industry standard XACML to incorporate TSCP requirements
- Launch efforts to standardize Microsoft groups around one policy definition language (SAML vs XRML)

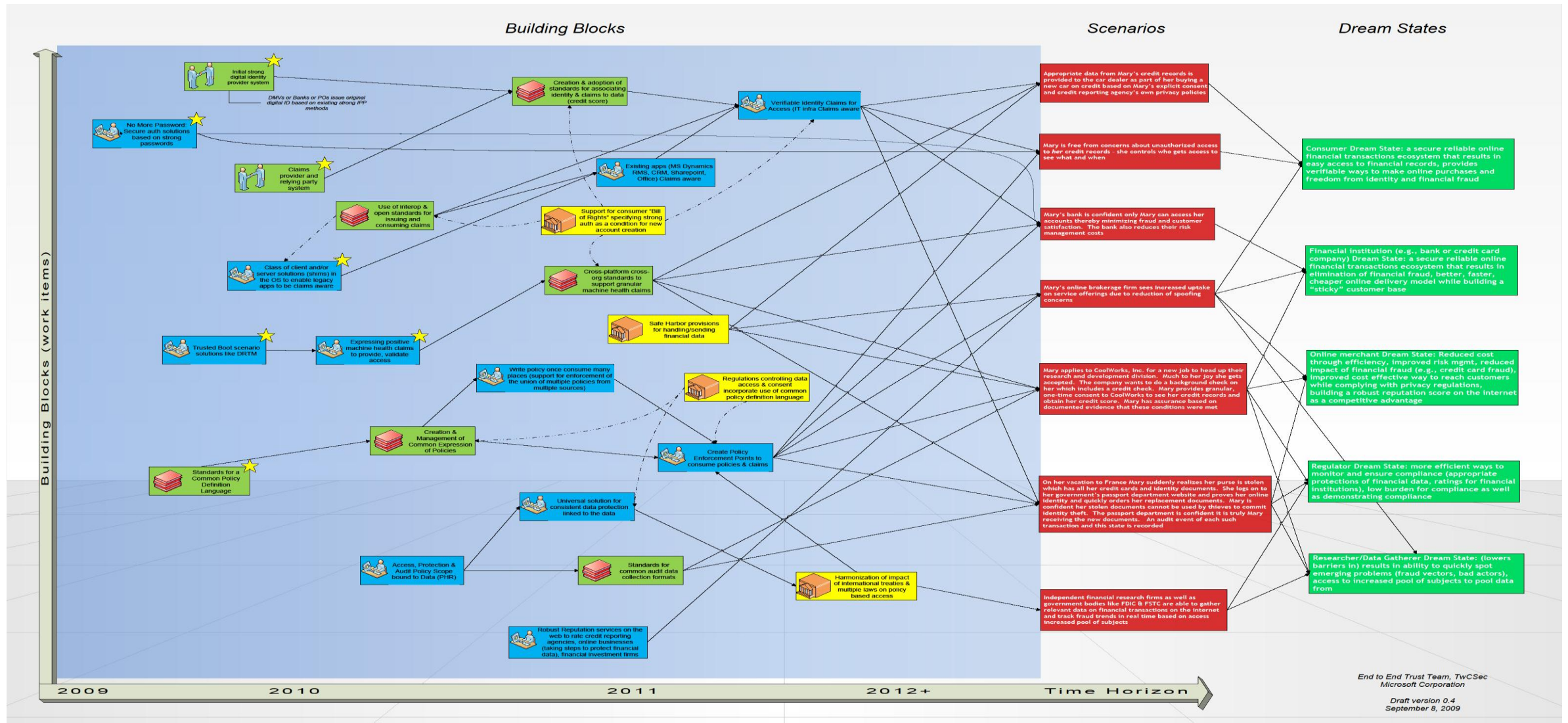
Step 2:

- Alternatives to XACML with a Microsoft and/or industry solution that has the right architecture to satisfy high level requirements for secure collaboration across v-orgs
- Work with the ecosystem partners to create/enhance standards for common policy definition language

Roadmap: Online Health Care High Value Internet Transactions



Roadmap: Financial High Value Internet Transactions



“Building Block” Families

System and Device Health

Digital Identity, Claims-based AuthN and AuthZ

Rule Based Data Access

Reputation Services

Verification (post-transactional, aka Audit)

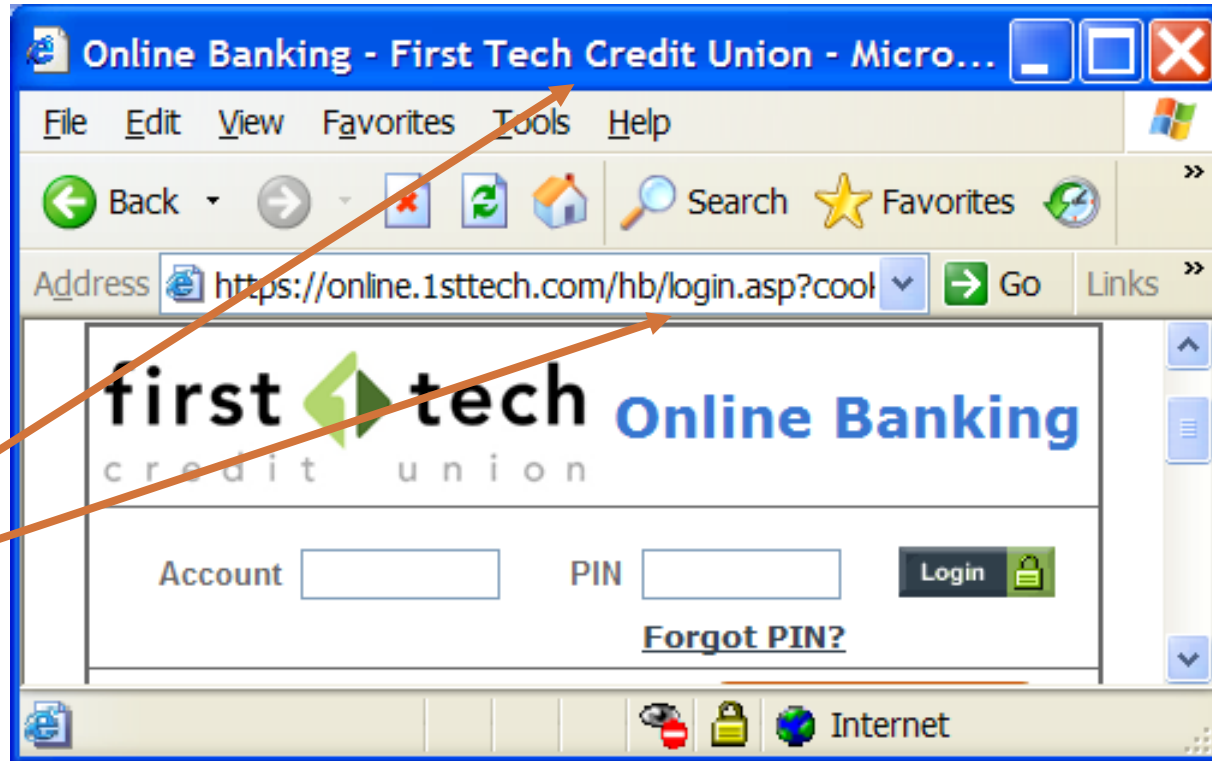
Trusted User Experience (TUX)

Assurance and Integrity

Trust User Experience (TUX)

- TUX is when you are put in the hot seat and need to make trust decision
 - Is this really your bank site
 - Is it OK to click on a link in your email
 - Is it safe to install new software?
 - Should I share my data?
 - How do I set the right permissions?
- Creating great TUX is hard and essential
- Must consider UI, underlying architecture, and user's mental model

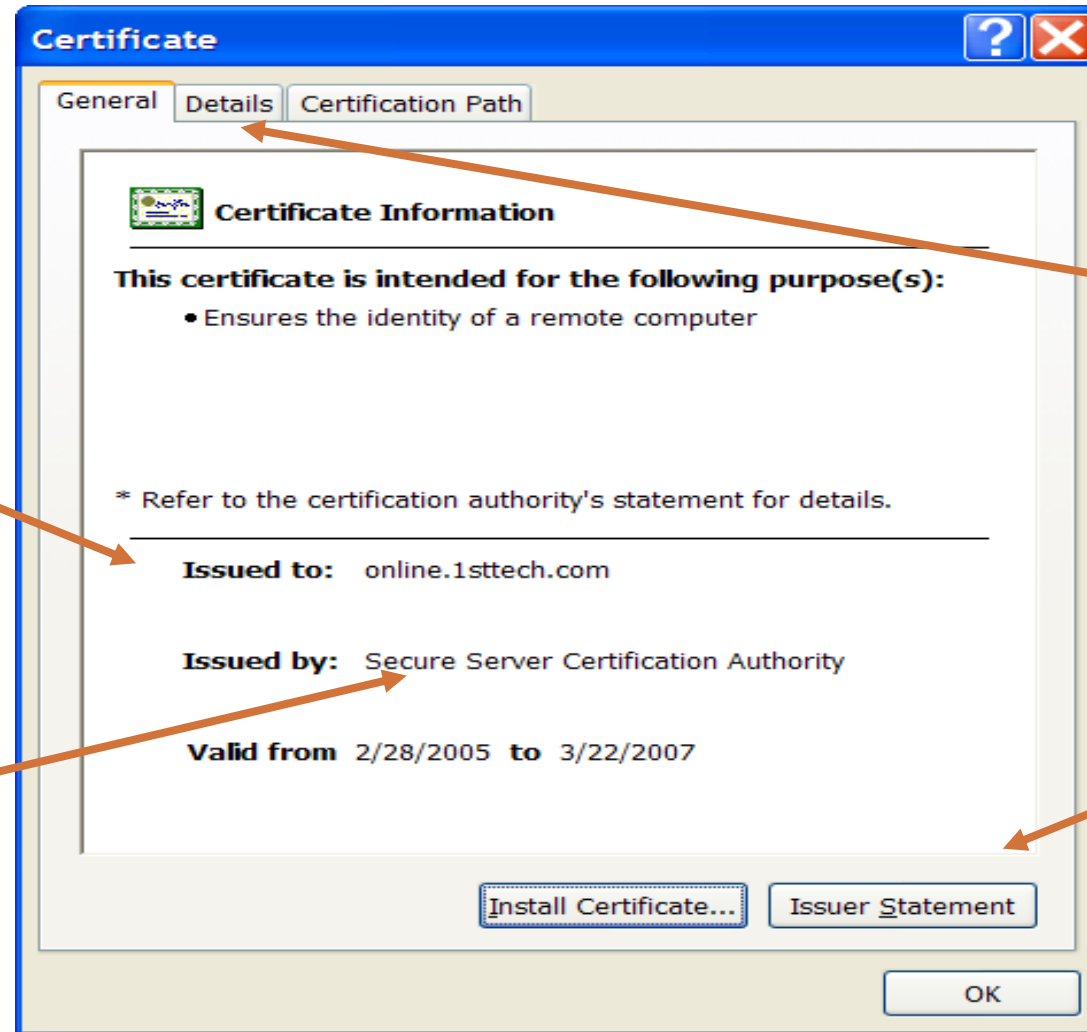
Login Please ...



Name is different, is that OK?

Has a "lock" but need to inspect – *bad guy can get one too!*

Have to Dig ...



Name of site, not organization

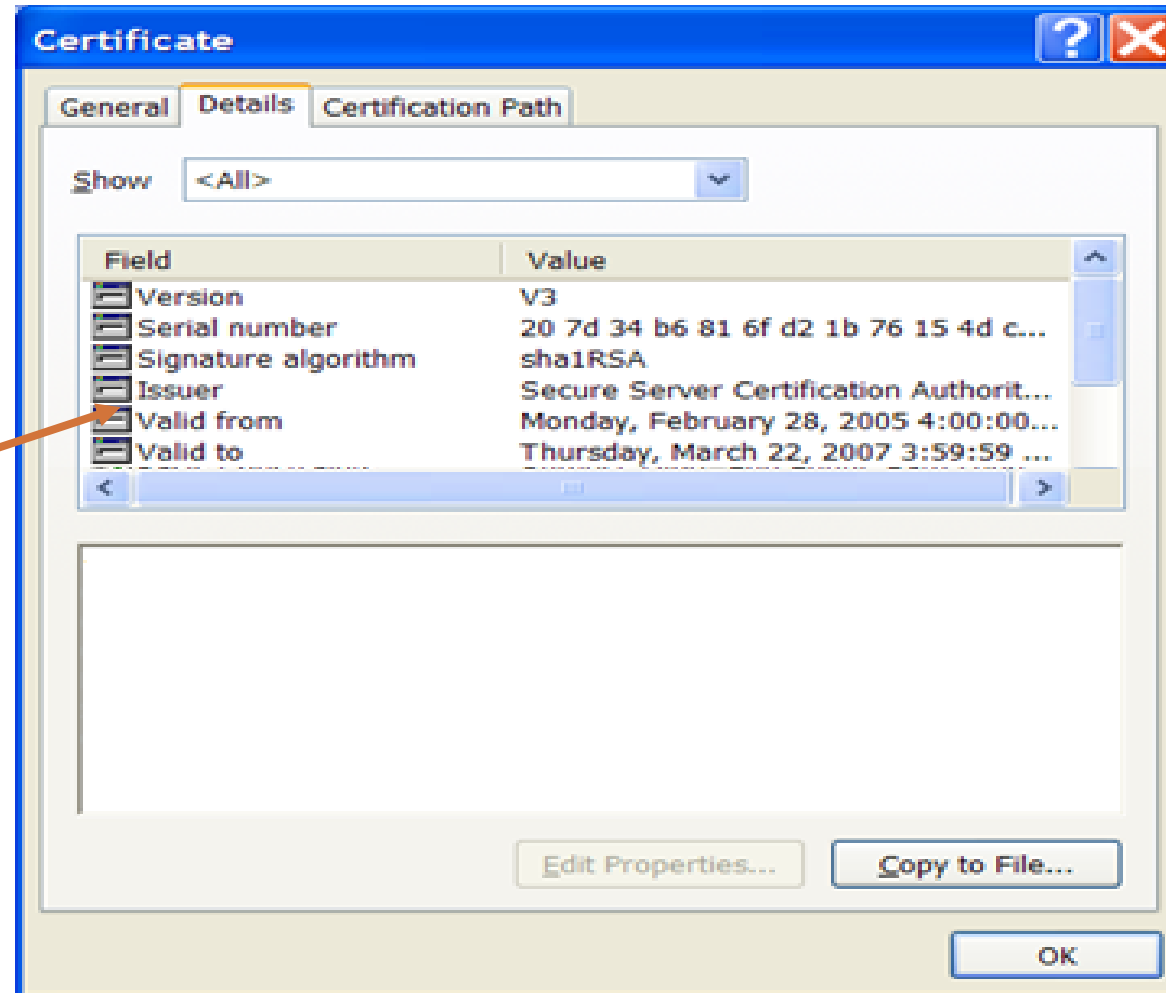
Should I trust this CA?
Not branded

Can click here to see additional information - *but it won't indicate which fields were verified by CA*

Have to click here to learn what checking was done - *no standard!*

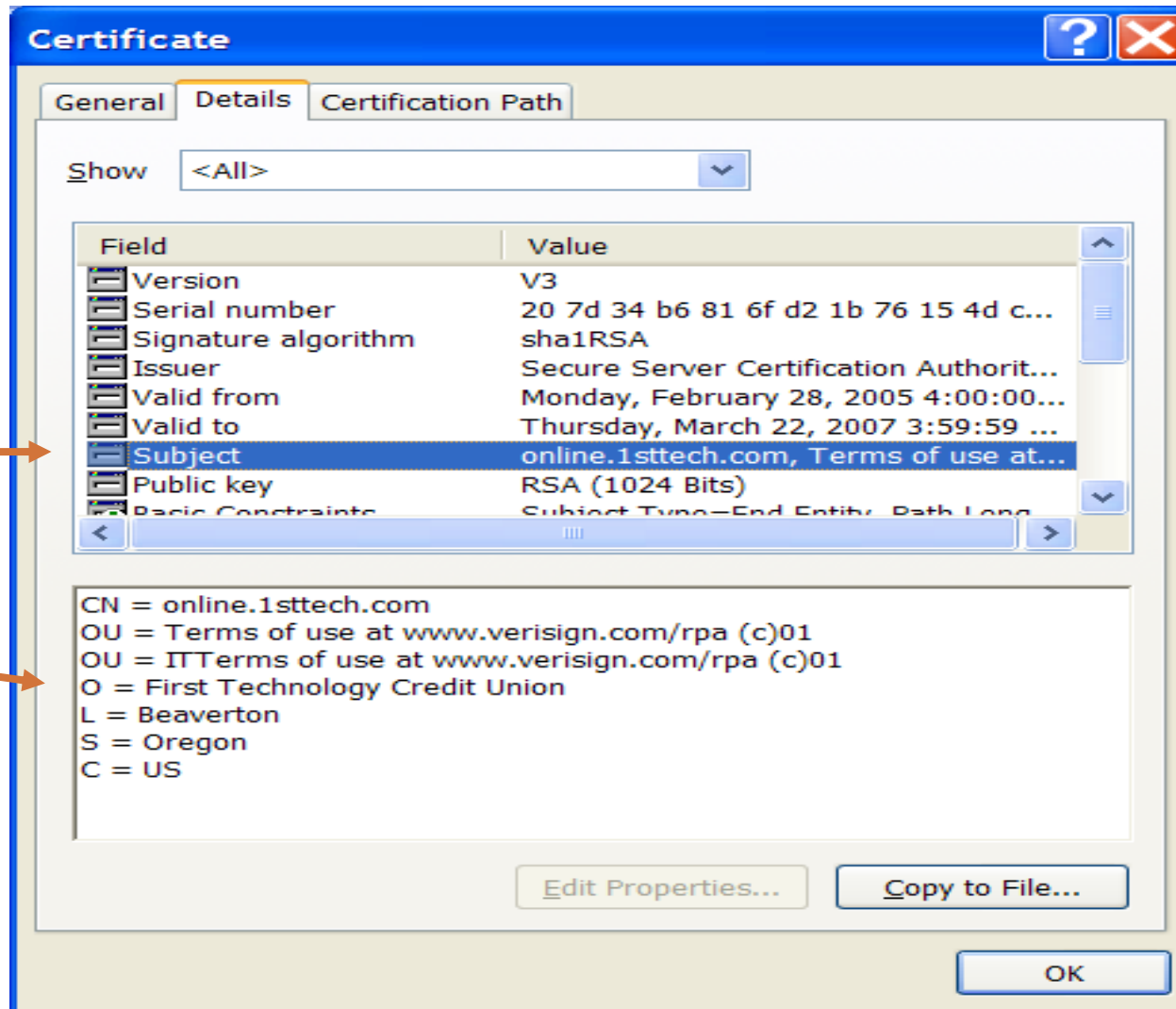
And Dig ...

Which field lists organization and location?

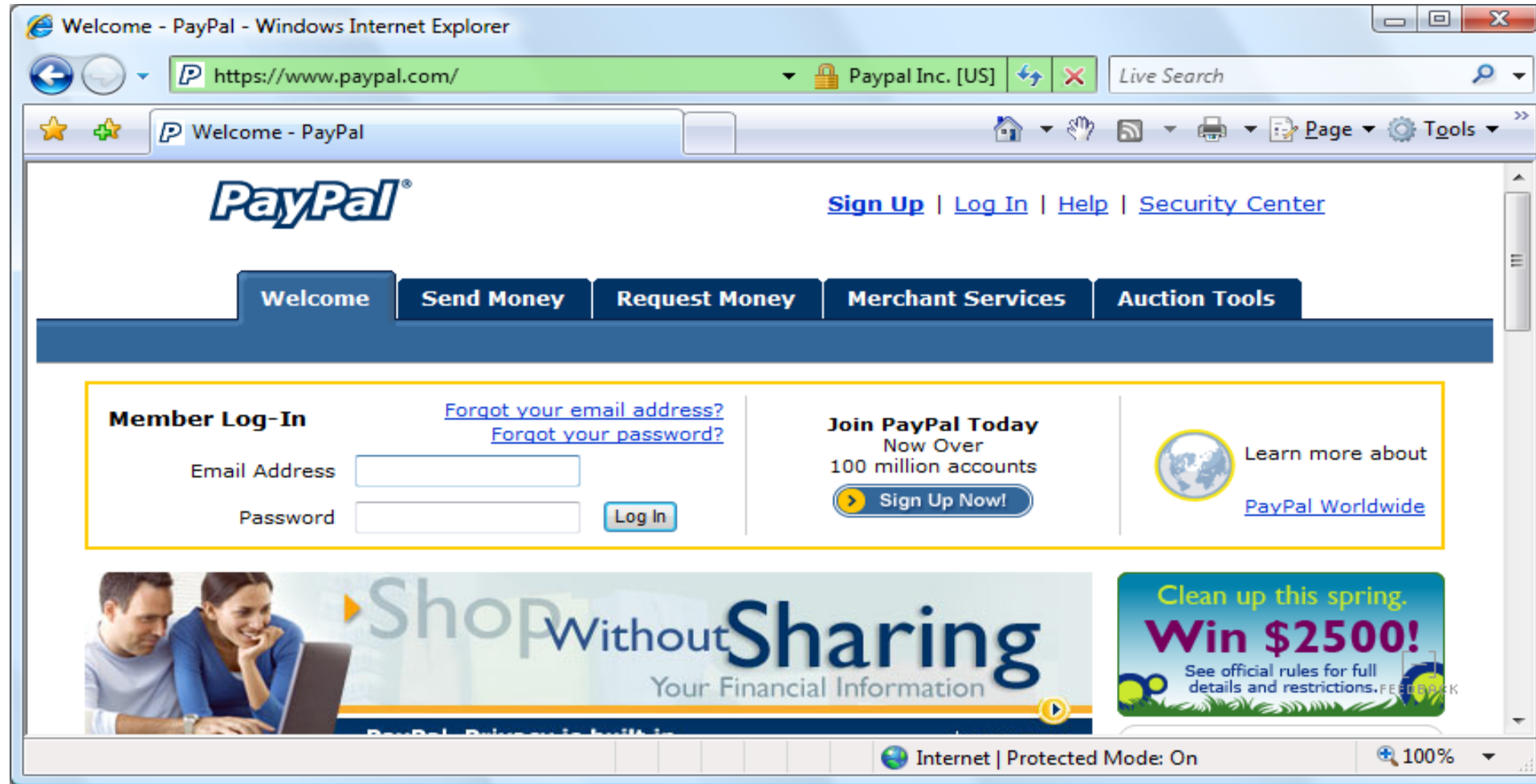


And Dig Some More ...

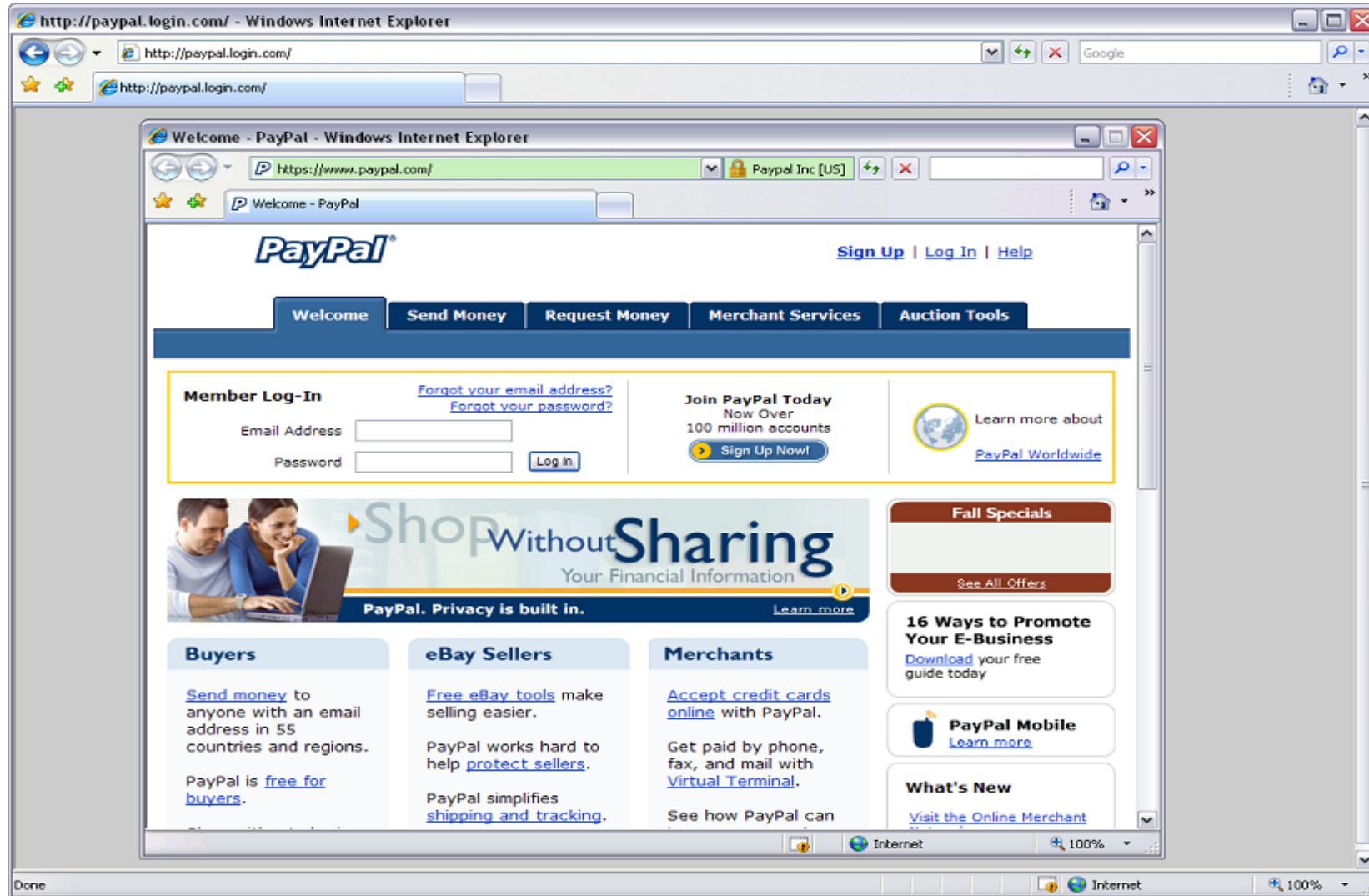
Need to click on
"Subject" to learn details
like organization or
location



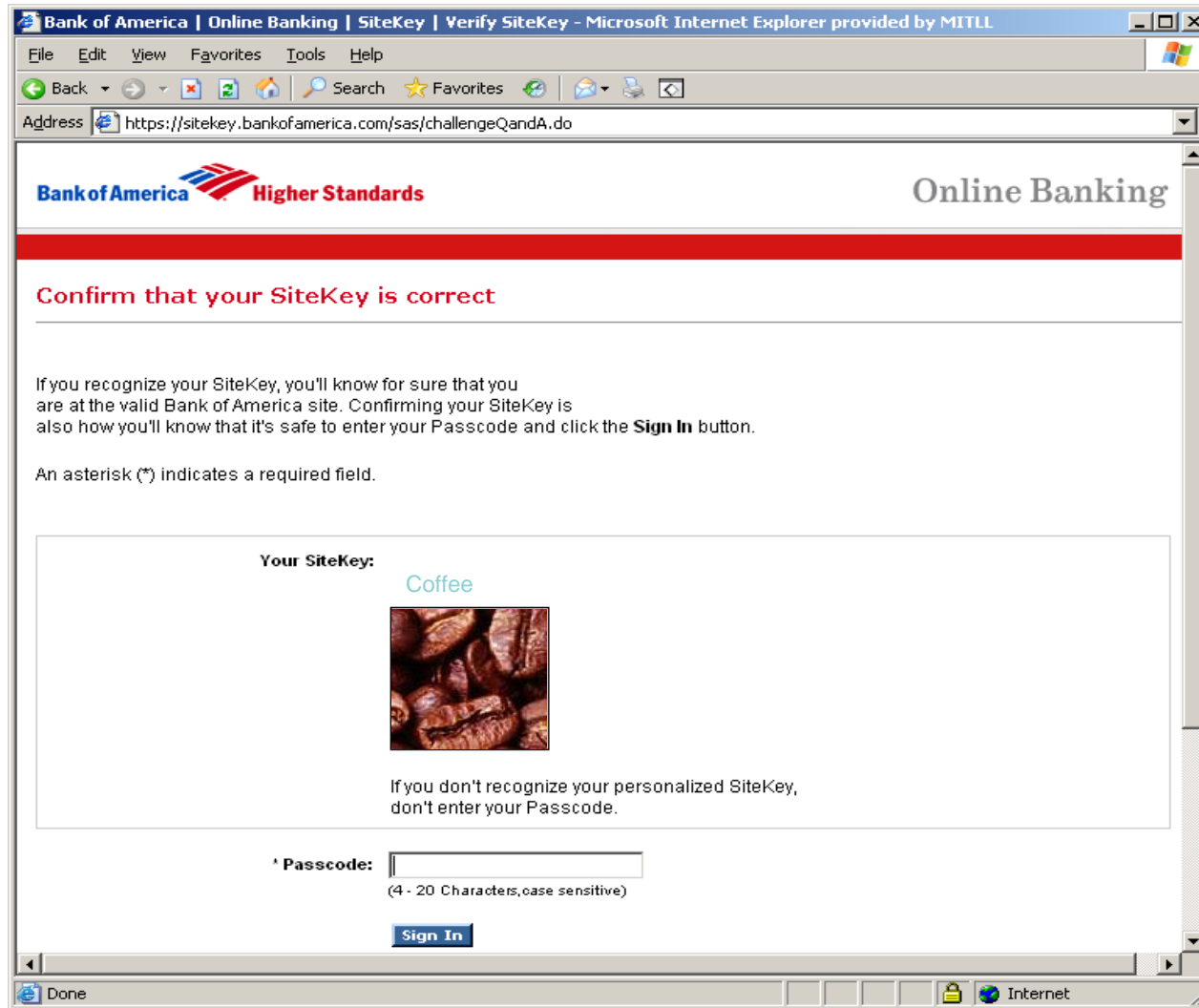
Better Mutual Authentication



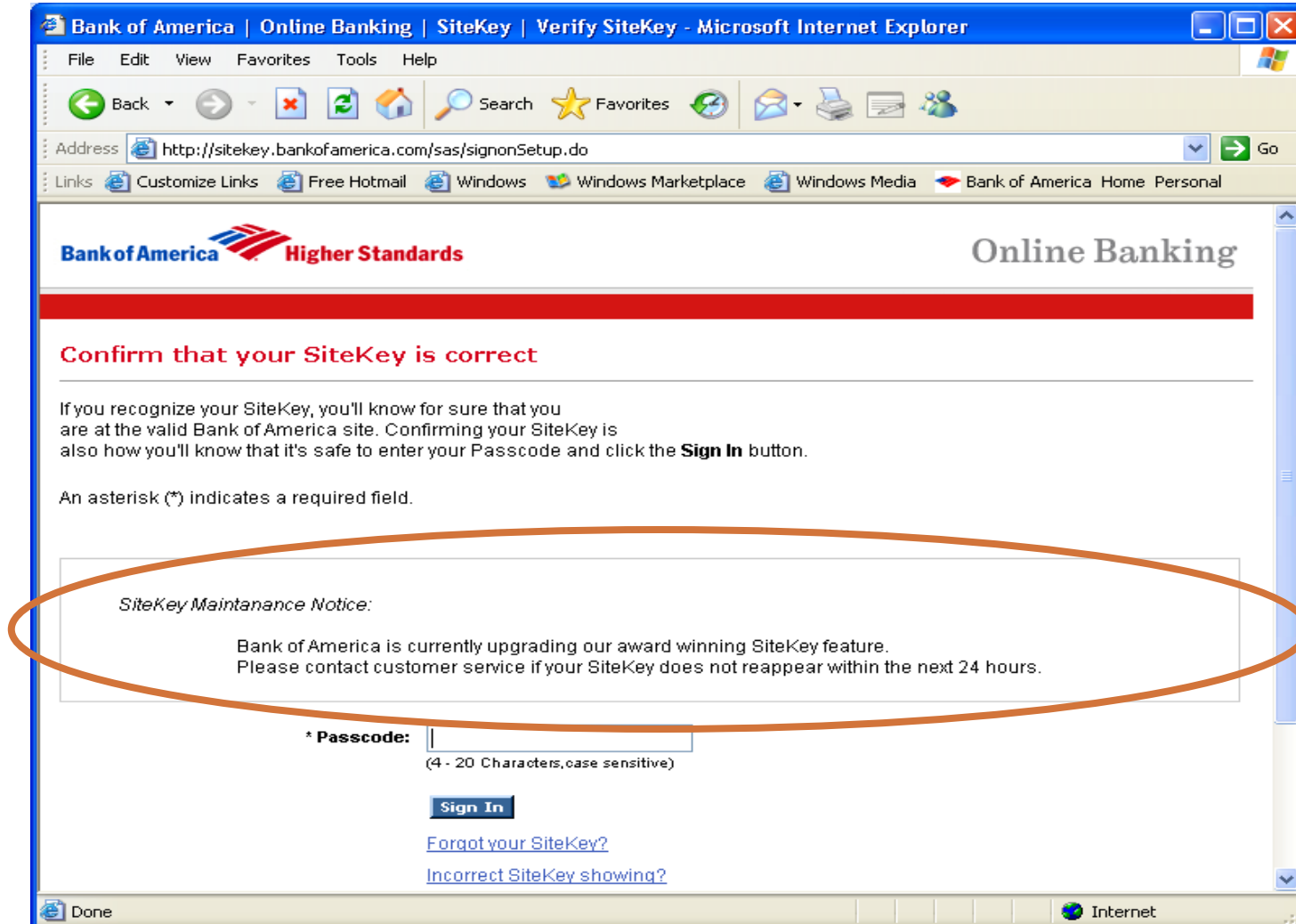
Picture in Picture Spoof



What About Visual Secrets?



Ignored by Almost All – 92%!



TUX Vision

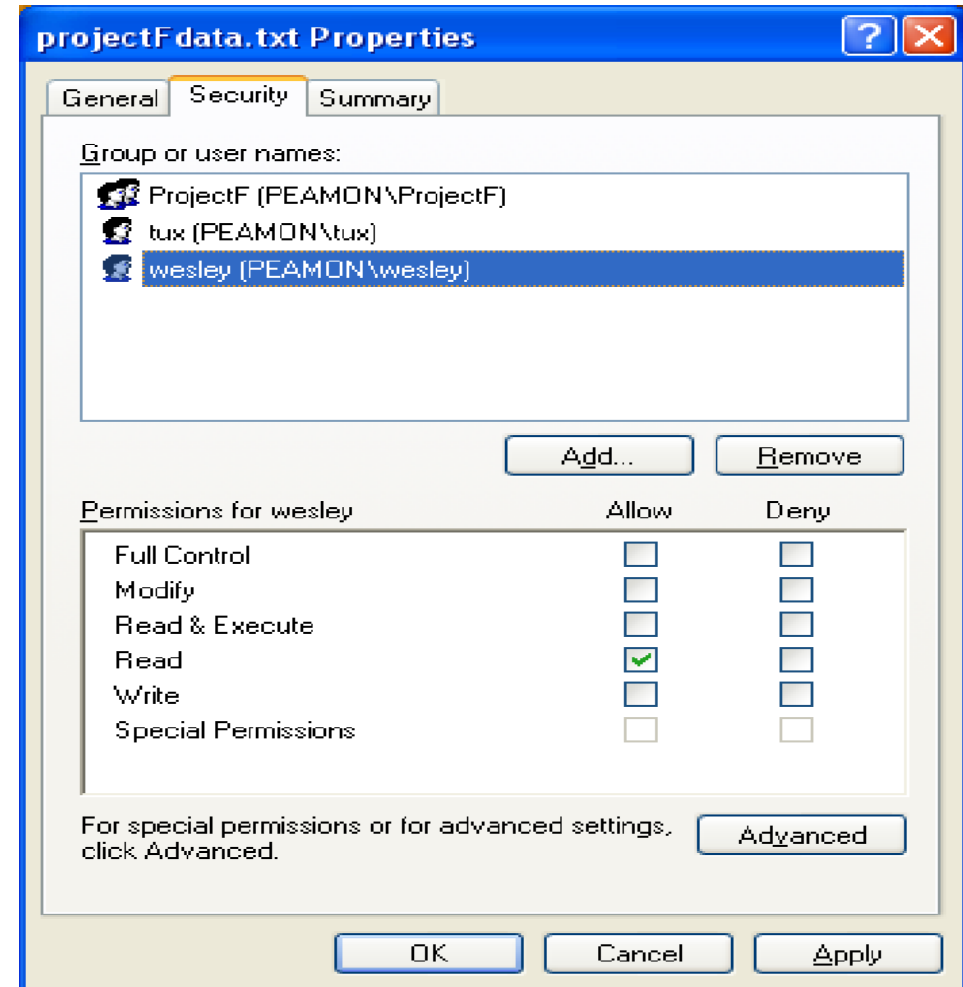
- Consumers
 - Safer, more confident
 - Not distracted from enjoying digital lifestyle
- Businesses
 - Better able to connect with customers, partners, and other businesses
 - Can honor trust promises, reduce breaches, and protect and build their brand

TUX Research Areas

- Authentication
 - Secret questions (IEEE Symposium on S&P 08)
 - Social Auth (CHI09)
 - Backup Auth Configuration (SOUPS09)
- End-user warning/consent
 - Application Authorization (submitted to CHI10)
- Access-control management
 - Laissez-faire file sharing (NSPW09)
 - Expandable Grid
 - Advanced Permissioning Experience

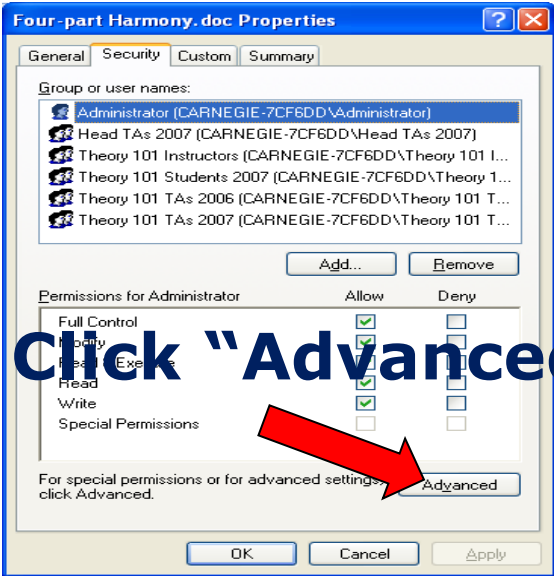
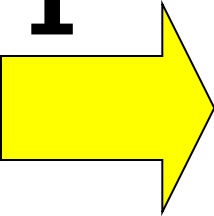
Access Control – Status Quo

- Use ACL Editor
- Really hard if groups and deny rules in play
- 19 screens!



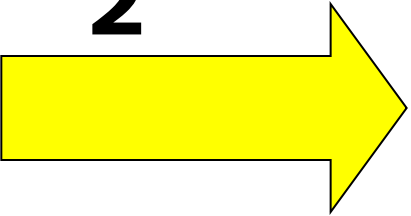
Inspect User Permissions

1

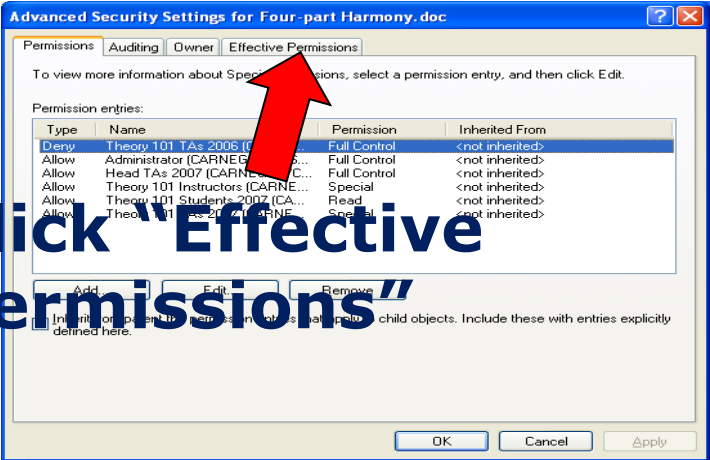


Click "Advanced"

2

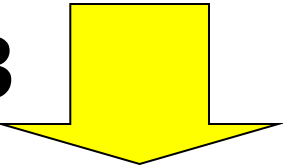


Click "Effective Permissions"

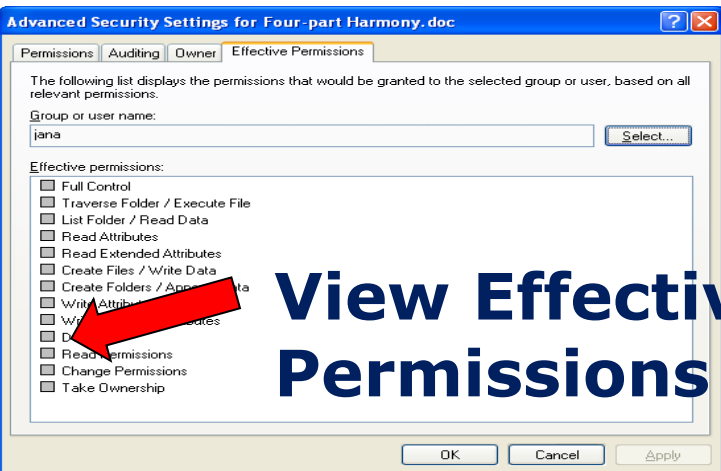


Type	Name	Permission	Inherited From
Deny	Theory 101 TAs 2006 (CARNE...	Full Control	<not inherited>
Allow	Administrator (CARNEGIE-7CF6DD\A...	Full Control	<not inherited>
Allow	Head TAs 2007 (CARNEGIE-7CF6DD\H...	Full Control	<not inherited>
Allow	Theory 101 Instructors (CARNEGIE-7CF6DD\T...	Special	<not inherited>
Allow	Theory 101 Students 2007 (CARNEGIE-7CF6DD\T...	Read	<not inherited>
Allow	Theory 101 TAs 2007 (CARNEGIE-7CF6DD\T...	Special	<not inherited>

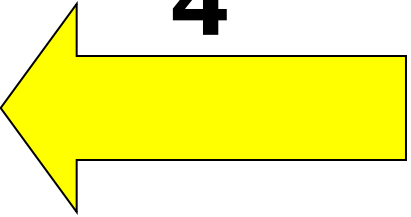
3




View Effective Permissions



4

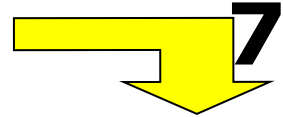
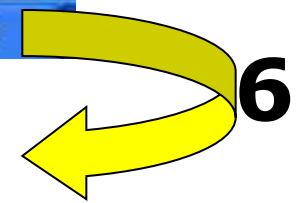
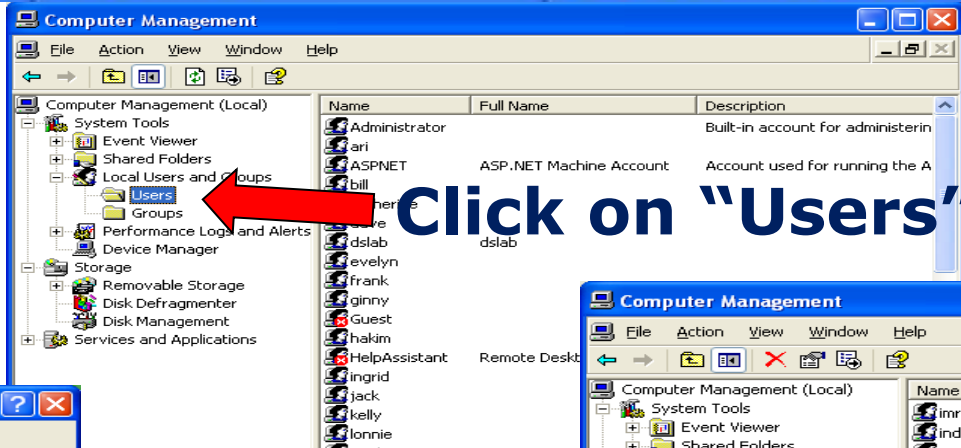
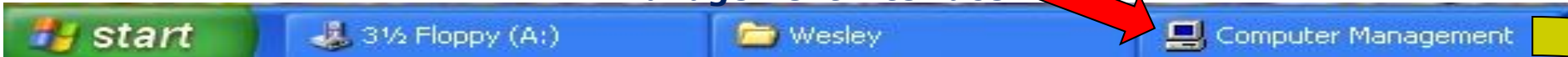
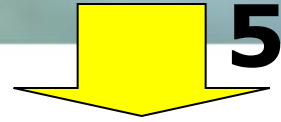


Select User

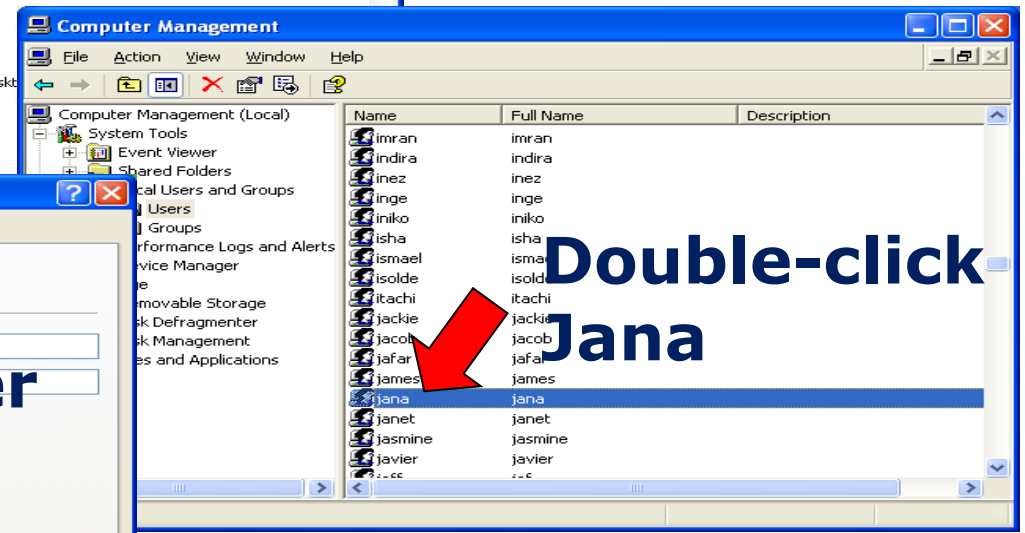


Inspect Group Membership

Bring up Computer Management interface



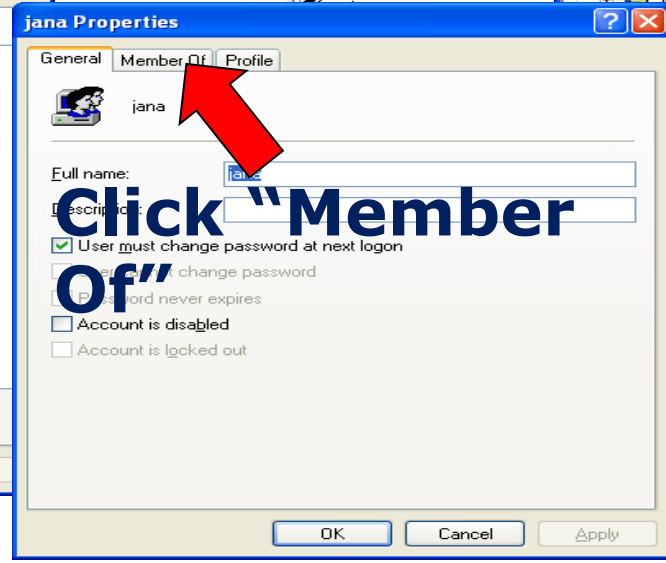
Click on "Users"



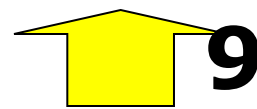
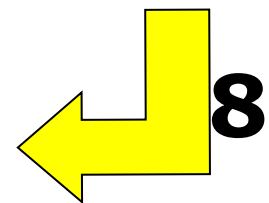
Double-click Jana



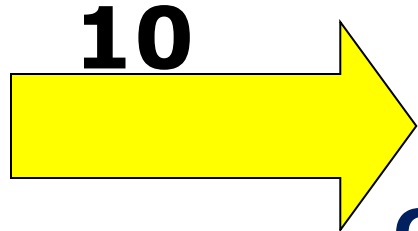
Read group membership



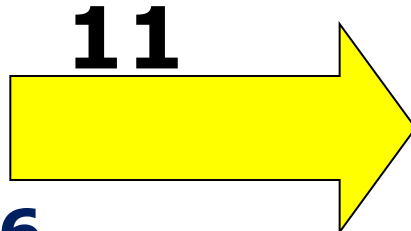
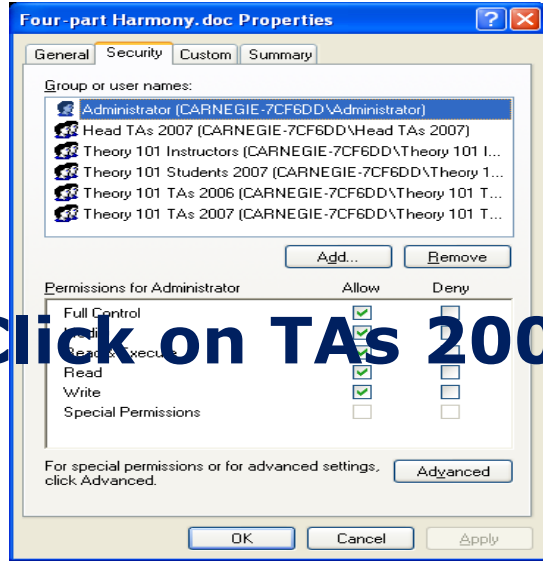
Click "Member Of"



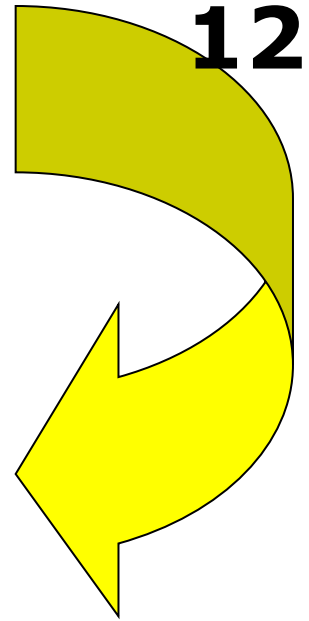
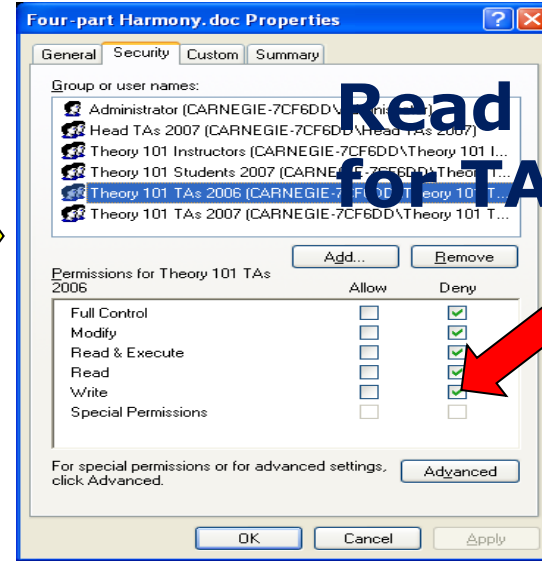
Inspect Group Permissions



Click on TAs 2006

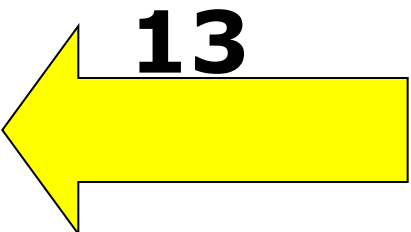
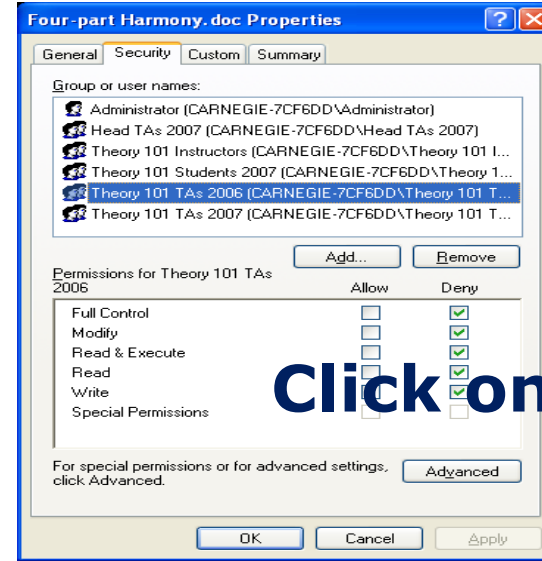


Read permissions for TAs 2006



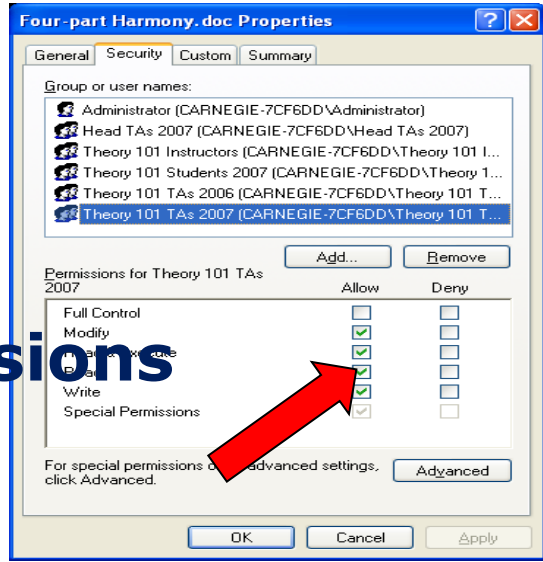
12

Click on TAs 2007



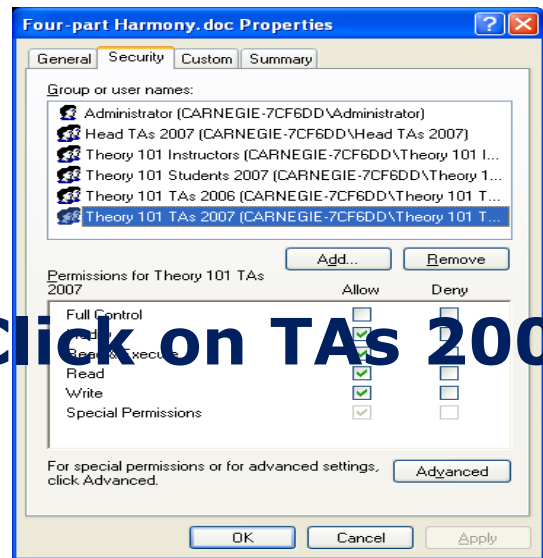
13

Read permissions for TAs 2007



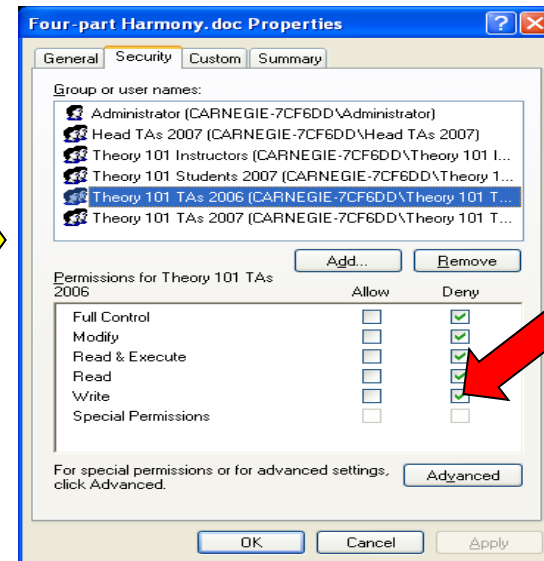
Change Group Permissions

14



Click on TAs 2006

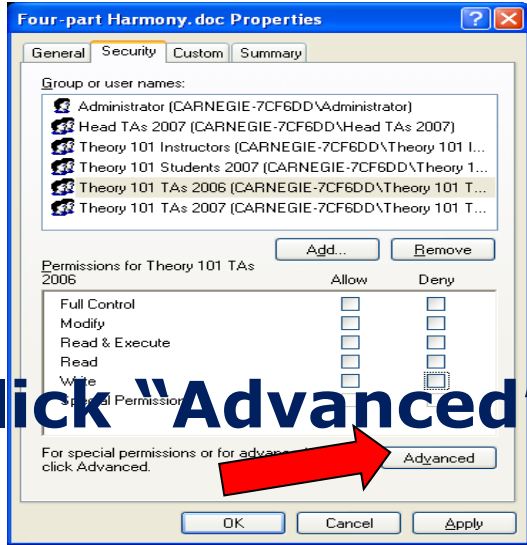
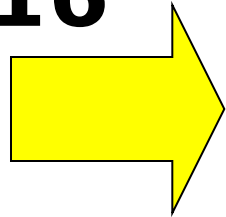
15



Change permissions for TAs 2006

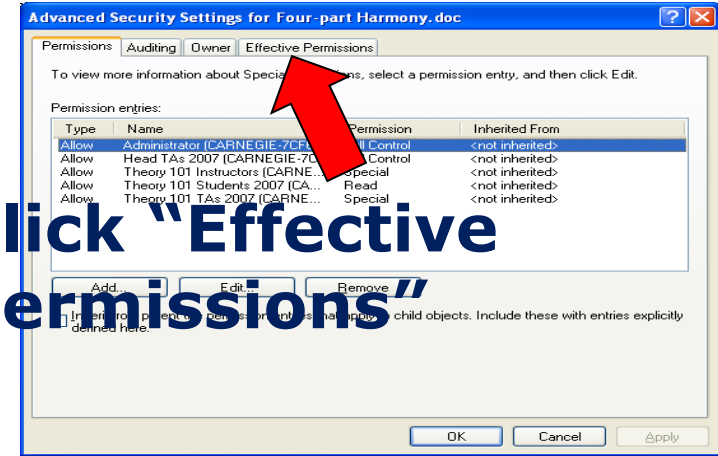
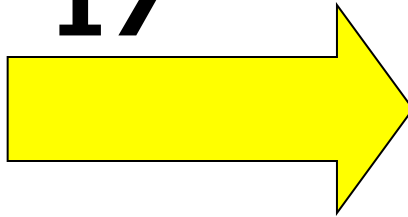
Check Your Work

16



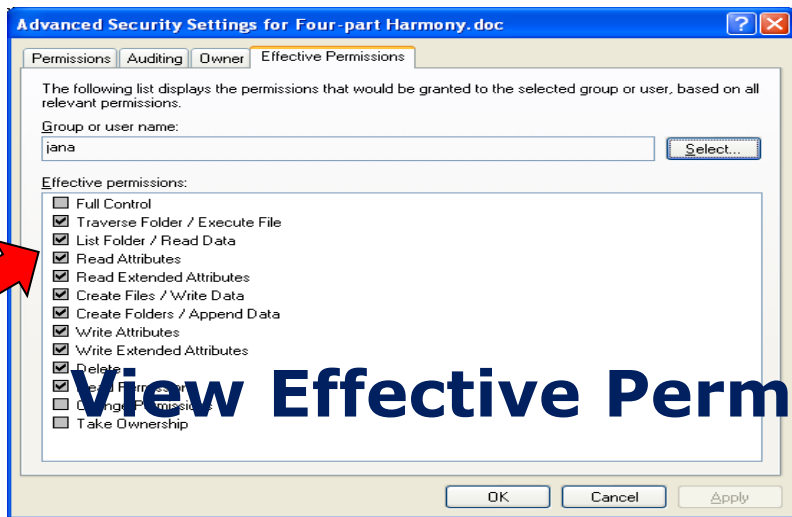
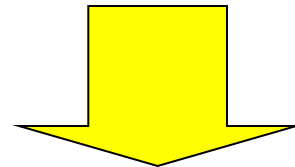
Click "Advanced"

17



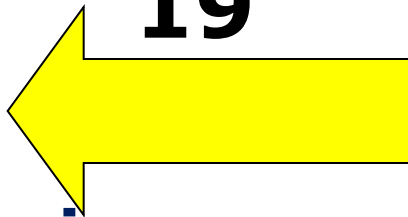
Click "Effective Permissions"

18



View Effective Permissions

19

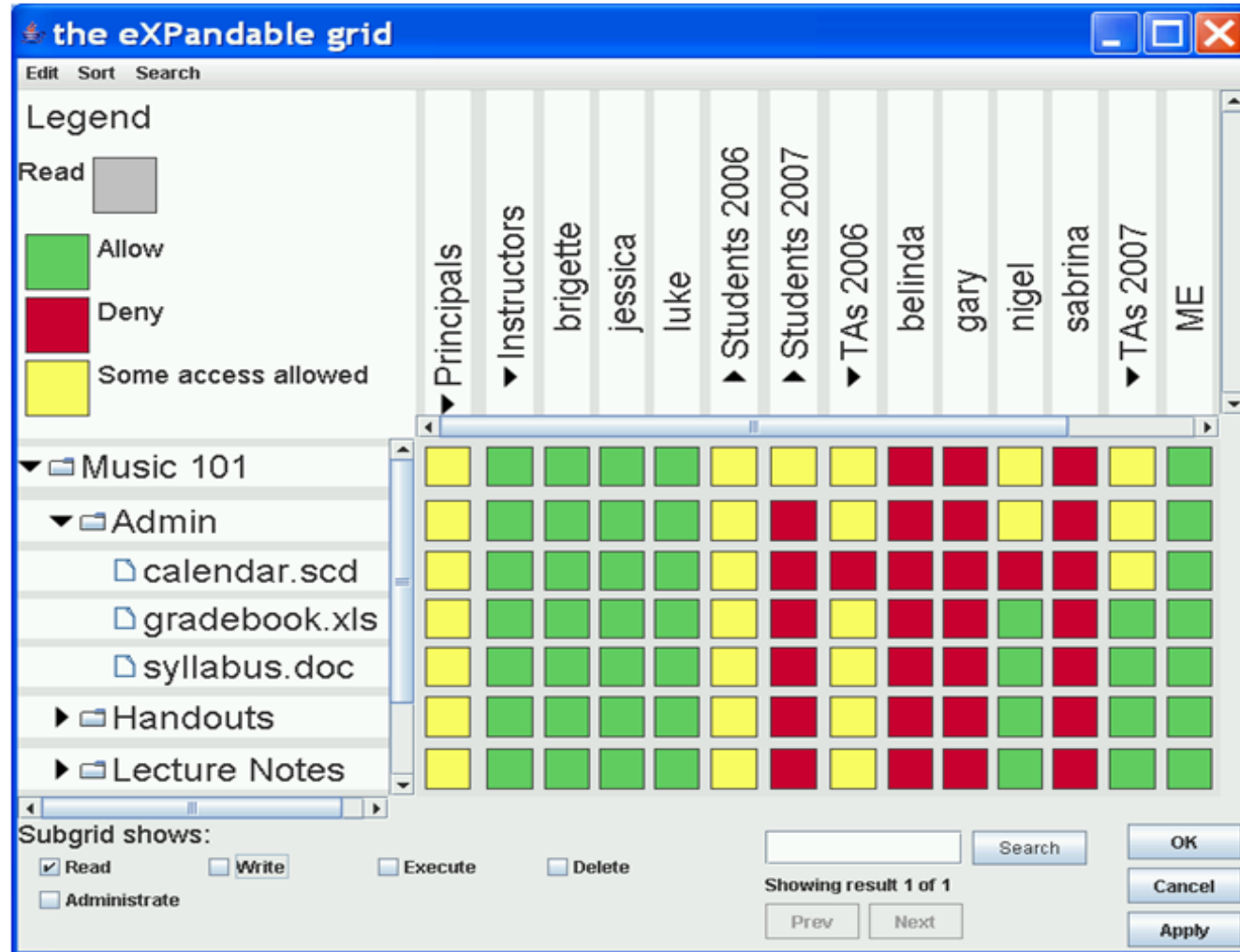


Select Jana

Challenges with ACL

- Key information is distributed
- Easy to make silly mistakes
- Need a way to directly check and manage permissions

Expandable Grid



Next level (if you need it)

The screenshot shows a window titled "the eXPandable grid" with a menu bar (File, Edit, Sort) and a legend. The legend defines permissions: Read, Write, Execute, Delete, and Administrate, each represented by a grid of squares. It also defines access levels: Allow (green), Deny (red), and Some access allowed (yellow). The main grid displays permissions for users: Theory 101 Students 2006, Theory 101 Students 2007, Theory 101 TAs 2006, chan, edna, henry, jana, kavita, Theory 101 TAs 2007, clayton, jana, and makana. A subgrid is expanded for the "Handouts" folder, showing permissions for files: Four-part Harmony.d, Musical Analysis1.doc, Musical Analysis2.doc, Pitch Training.doc, Simple Harmony.doc, and Simple Solo.doc. The subgrid shows checked permissions for Read, Write, Execute, Delete, and Administrate. A search box and "Search" button are present, along with "Prev" and "Next" navigation buttons.

File/Folder	Theory 101 Students 2006	Theory 101 Students 2007	Theory 101 TAs 2006	chan	edna	henry	jana	kavita	Theory 101 TAs 2007	clayton	jana	makana
Handouts	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Four-part Harmony.d	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Musical Analysis1.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Musical Analysis2.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Pitch Training.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Simple Harmony.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow
Simple Solo.doc	Some access allowed	Some access allowed	Deny	Deny	Deny	Deny	Deny	Deny	Some access allowed	Allow	Deny	Allow

And the winner is ...

Task type	Small-size		Large-size	
	Accuracy	Time	Accuracy	Time
<i>View simple</i>	 89% 56%	 29s 64s	 61% 56%	 42s 61s
<i>View complex</i>	 94% 17%	 35s 55s	 100% 39%	 39s 67s
<i>Change simple</i>	 89% 94%	 30s 52s	 100% 100%	 50s 42s
<i>Change complex</i>	 61% 0%	 70s Insufficient data	 67% 17%	 100s 143s
<i>Change complex</i>	 89% 83%	 39s 103s	 67% 83%	 73s 104s
<i>Compare groups</i>	 67% 61%	 55s 103s	 72% 61%	 73s 104s
<i>Conflict simple</i>	 89% 0%	 29s Insufficient data	 100% 6%	 52s Insufficient data
<i>Conflict complex</i>	 100% 94%	 20s 66s	 94% 78%	 105s 116s
<i>Memogate simulation</i>	 89% 94%	 42s 118s	 78% 78%	 71s 115s
<i>Precedence rule test</i>	 100% 100%	 100s 100s	 100% 100%	 100s 100s

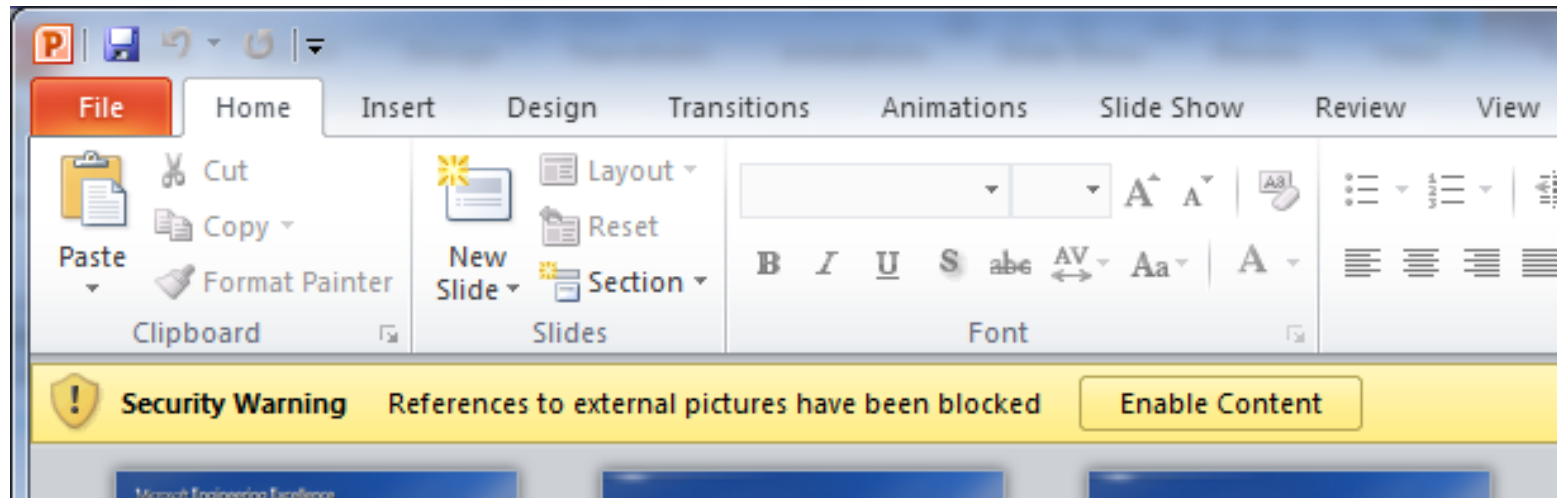
Secret questions

(IEEE Symposium on Security and Privacy 2009)

	Statistically guessable	Guessed by untrusted partner	
Forget			<i>Fact-based questions</i>
32%	14%	18%	Grandfather's occupation
35%	23%	17%	Favorite historical person
14%	10%	17%	Mother's birthplace
5%	5%	12%	What is your father's middle name?
17%	—	5%	What was your first phone number?
9%	1%	8%	What was the name of your first school?
21%	8%	13%	Where was your first job?
			<i>Preference-based questions</i>
18%	1%	11%	Best childhood friend
21%	—	4%	Favorite teacher
25%	6%	7%	What is your favorite restaurant?
15%	1%	8%	Who is your favorite singer?

Warnings – Latest Thinking

- No TUX is good TUX
- If you have to warn, be safe by default and don't interrupt



- If you have to interrupt, give users realistic steps they can follow

Open Questions

- Does an interruptive warning, when well-written and actionable, actually help users avoid attacks?
- What can we realistically ask users to decide?
- When should we warn versus just take action?

- What is the sweet spot for “informed consent” and how do we get there?

- How do we facilitate minimal disclosure?

Want to Learn More?

- End to End Trust
 - <http://www.microsoft.com/endtoendtrust>
- Symposium on Usable Privacy and Security (SOUPS)
 - At the Microsoft commons 7/14-7/16
- Jeff's Email Address
 - Jeffreyf@microsoft.com

The Microsoft logo is centered on the page. It consists of the word "Microsoft" in a bold, italicized, black sans-serif font. A registered trademark symbol (®) is located at the top right of the word.

© 2010 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

Microsoft® Research

Faculty Summit 2010