



University of British Columbia

Secure Web 2.0 Content Sharing Beyond Walled Gardens

San-Tsai Sun, Kirstie Hawkey, Konstantin Beznosov

Department of Electrical and Computer Engineering
Laboratory for Education and Research in Secure Systems Engineering (**LERSSE**)

outline

- overview
- approach
- implementation
- conclusion

Web 2.0: user-centric Web

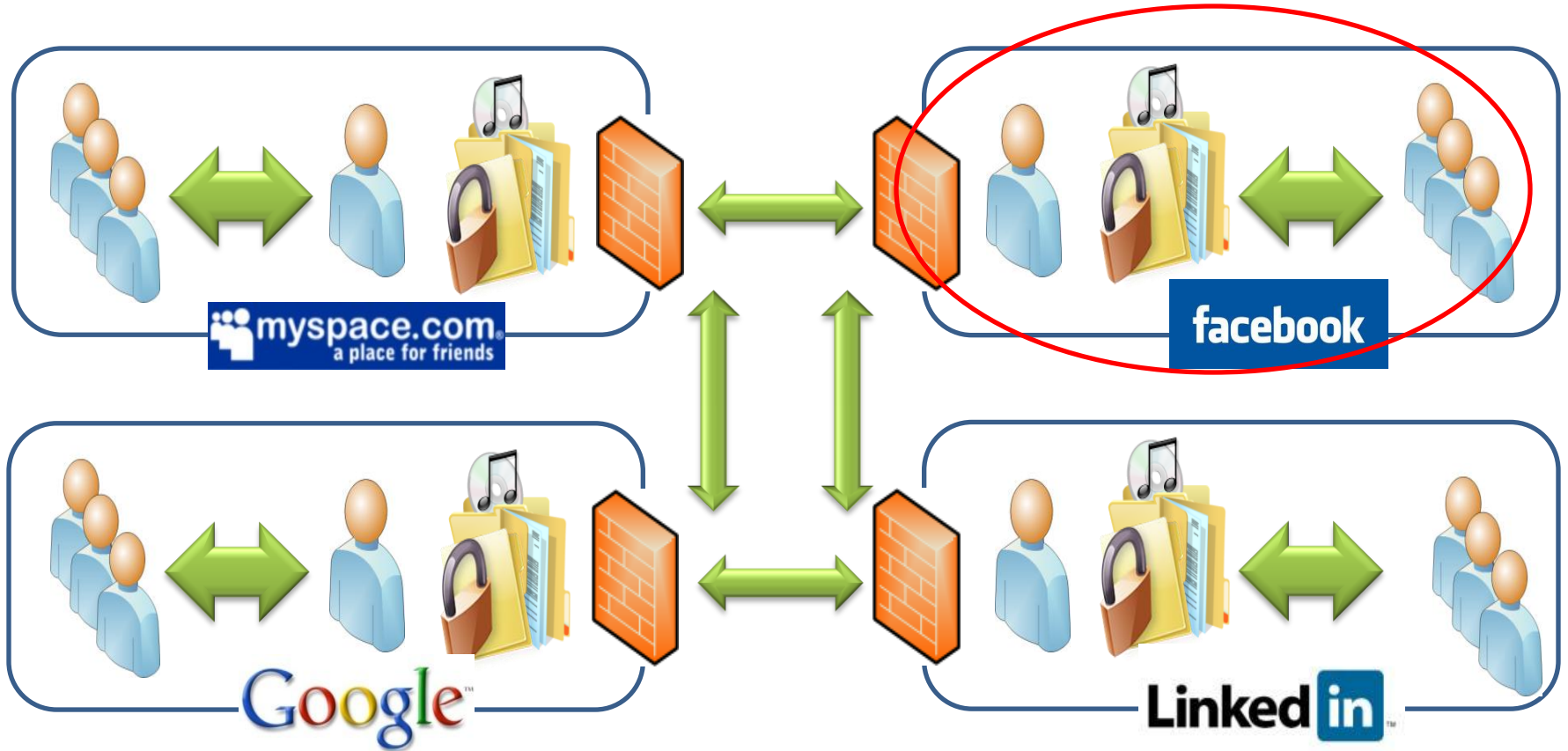


"Web 2.0 is a very different thing. It's a tool for bringing together the small contributions of millions of people and making them matter."

Lev Grossman, "Time's Person of the Year: You," in Time Magazine. Wednesday, Dec. 13, 2006.

Dec. 2006

walled garden problem



lack of usable mechanisms for secure Web 2.0 user
content sharing across
content and service providers (CSPs)

content sharing scenario

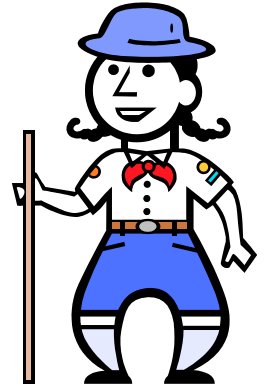


CCA scouts only

Canadian Coast Adventures (CCA)
Girl Scouts



Jenny



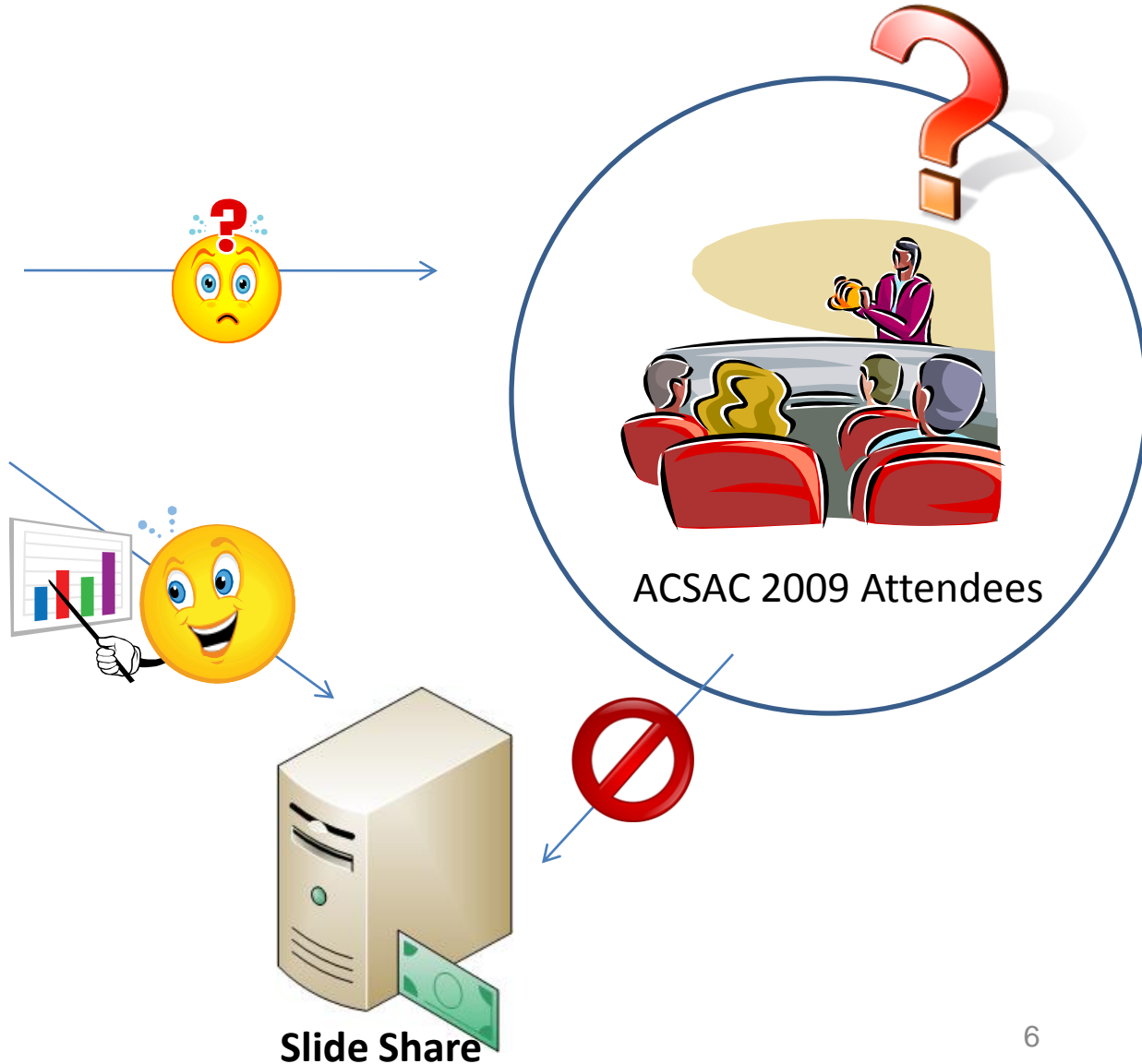
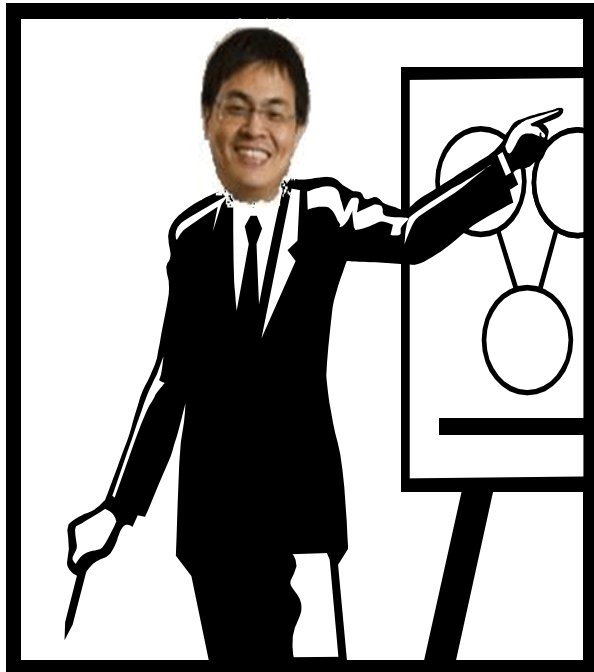
Alice



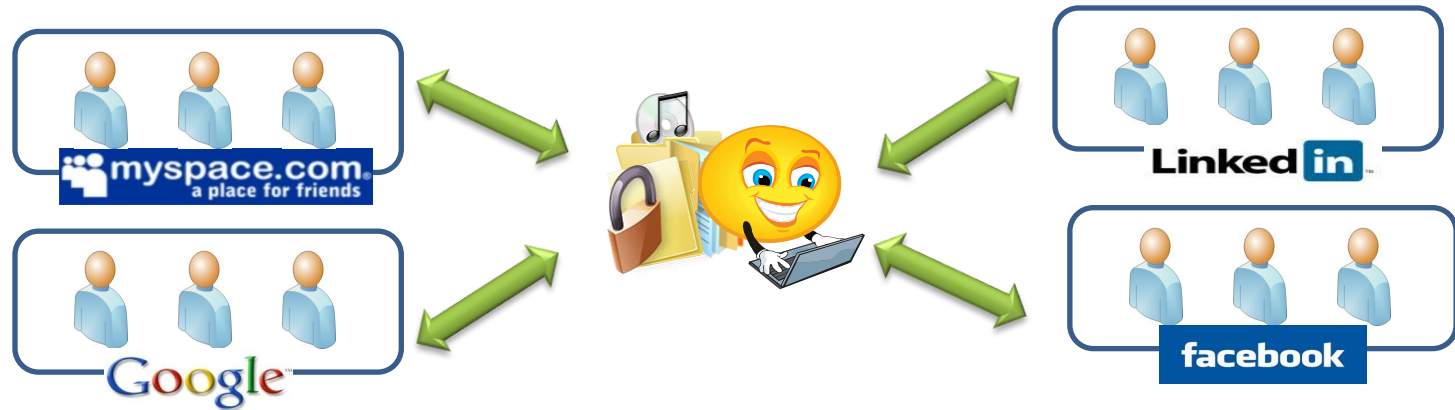
Picasa Web



sharing content with unknown user



research goal



Web-based content sharing mechanism

- ✓ enable users to share content with unknown Web users
- ✓ work beyond walled gardens

investigate the applicability of existing access-control systems when apply them to realize **user-centric policy** in the Web

challenges

- usability - usable for average Web users

Eric Sachs (product manager for Google security and internal systems),

"Redirects to login pages are bad, or are they?"

in SOUPS 2009 Keynote speaker, Mountain View, CA, USA. July 15-17, 2009.

“ designing hard to use security is easy
designing easy to use security is hard”

- interoperability
 - work across CSPs boundaries
 - work under current walled garden restrictions

usability

- user-centric
 - use the same identity and access policy across CSPs
- sharing experiences should be similar to users' existing file/content practices
- only use browser, no special software installed or crypto operations performed by user

interoperability

- build upon open standards and protocols
- for CSPs
 - provide additional content sharing channel
 - not required to change their existing access-control mechanism

existing secret-link approach

<http://picasaweb.google.com/Alice?authkey=Gv1sRgCOzuv>



Jenny



secret-link

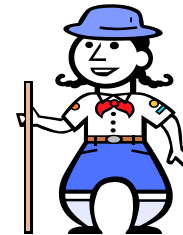
secret-link



Picasa Web



← jenny@aol.com —



Alice

- ✓ usable for Web users
- ✓ easy to implement by CSPs
- ✗ Alice does not have control over Jenny's sharing of secret link with others
- ✗ Alice has to know Jenny's email

content sharing user studies

- email is the most commonly used sharing mechanism [2,3,4,5]
- users tend to treat socially-defined classes of individuals the same when sharing [1,2,3]

[1] J. S. Olson, J. Grudin, and E. Horvitz, "A study of preferences for sharing and privacy," in CHI '05 extended abstracts on Human factors in computing systems (CHI '05). New York, NY, USA: ACM, 2005, pp. 1985–1988.

[2] S. Volda, W. K. Edwards, M. W. Newman, R. E. Grinter, and N. Ducheneaut, "Share and share alike: exploring the user interface affordances of file sharing," in Proceedings of the SIGCHI conference on Human Factors in computing systems CHI '06:. New York, NY, USA: ACM, 2006, pp. 221–230.14

[3] T. Whalen, "Supporting file sharing through improved awareness," Ph.D. Dissertation, Dalhousie University, Canada, 2008. [Online]. Available: <http://www.proquest.com/>

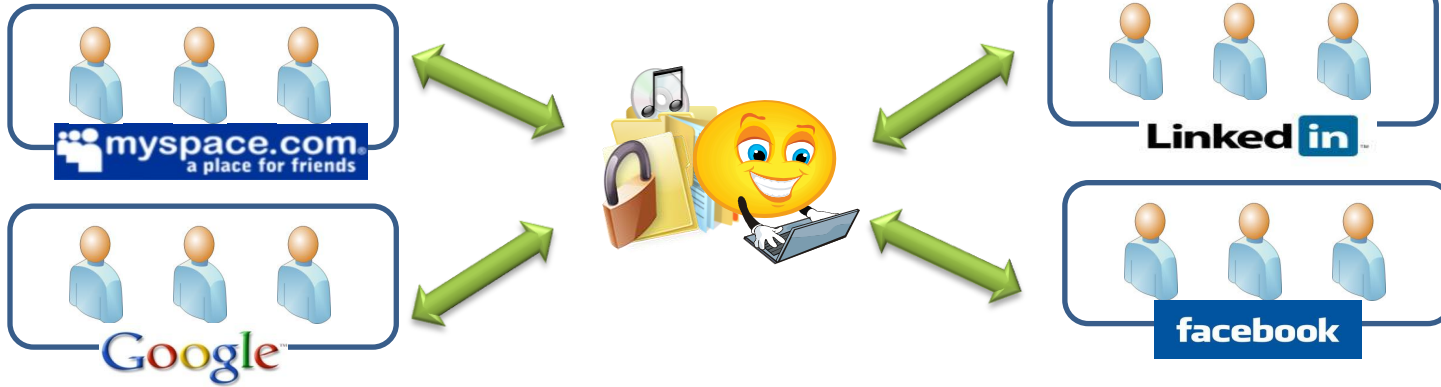
[4] N. A. Van House, "Flickr and public image-sharing: distant closeness and photo exhibition," in CHI '07: Ext. Abstracts on Human factors in computing systems. NY, NY, USA: ACM, 2007, pp. 2717–2722.

[5] A. D. Miller and W. K. Edwards, "Give and take: A study of consumer photo-sharing culture and practice," in Proceedings of the CHI 2007, San Jose, California, USA, April 28 –May 3 2007, pp. 347–356.

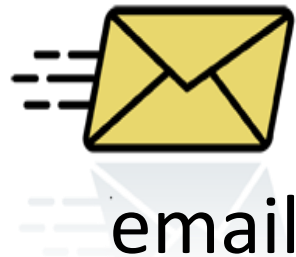
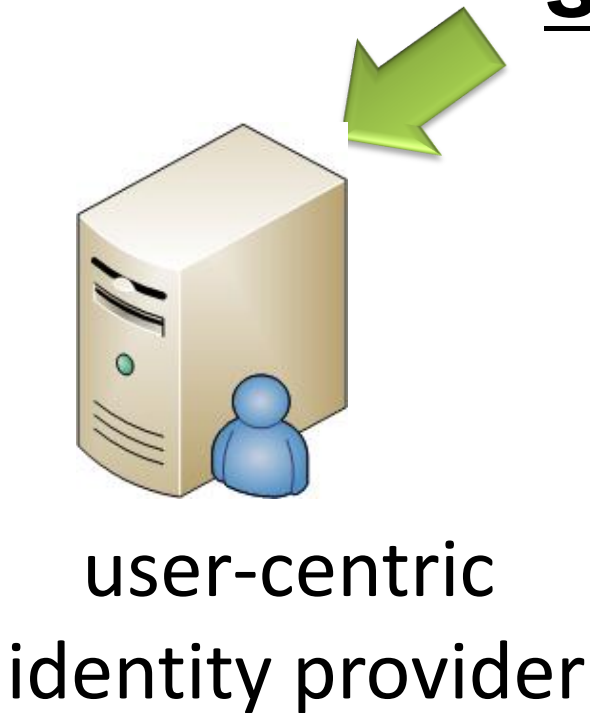
outline

- overview
- **approach**
- implementation
- conclusion

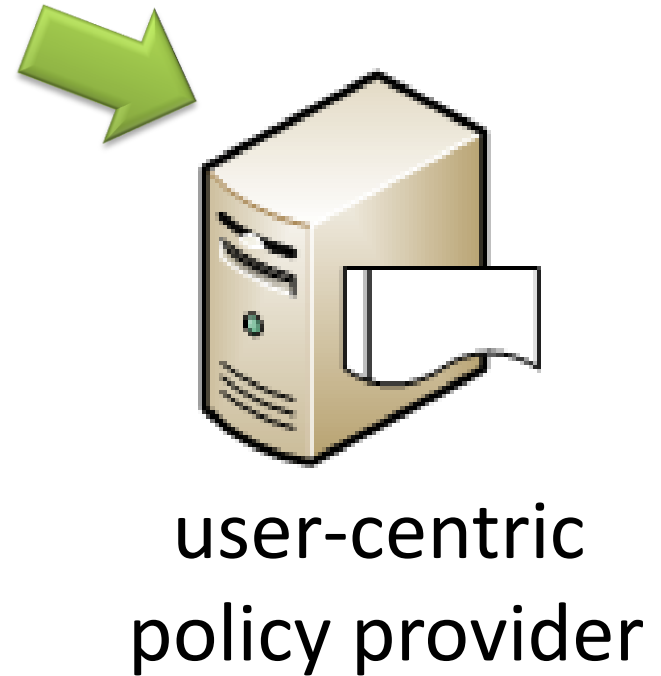
ideas



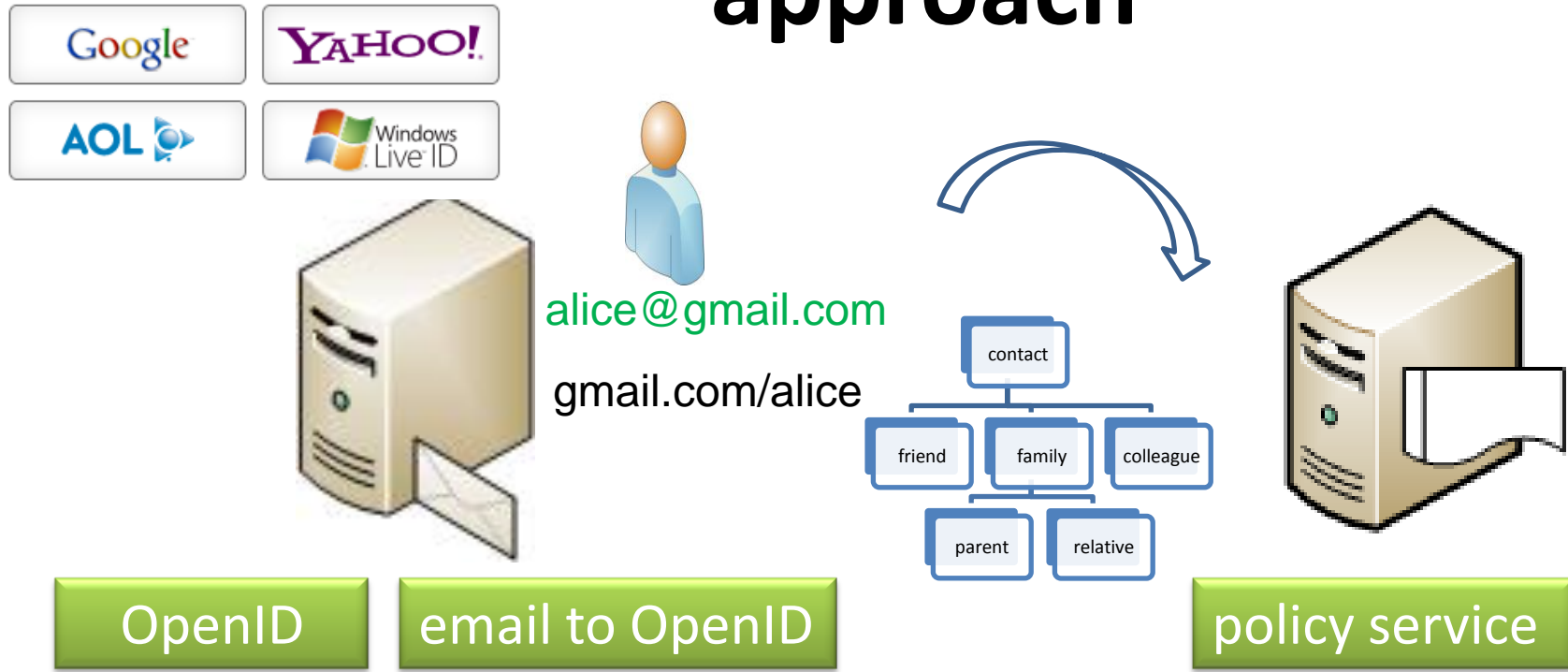
secret-link



email



approach



OpenID

email to OpenID

policy service

enables users to use their email
to login CSPs

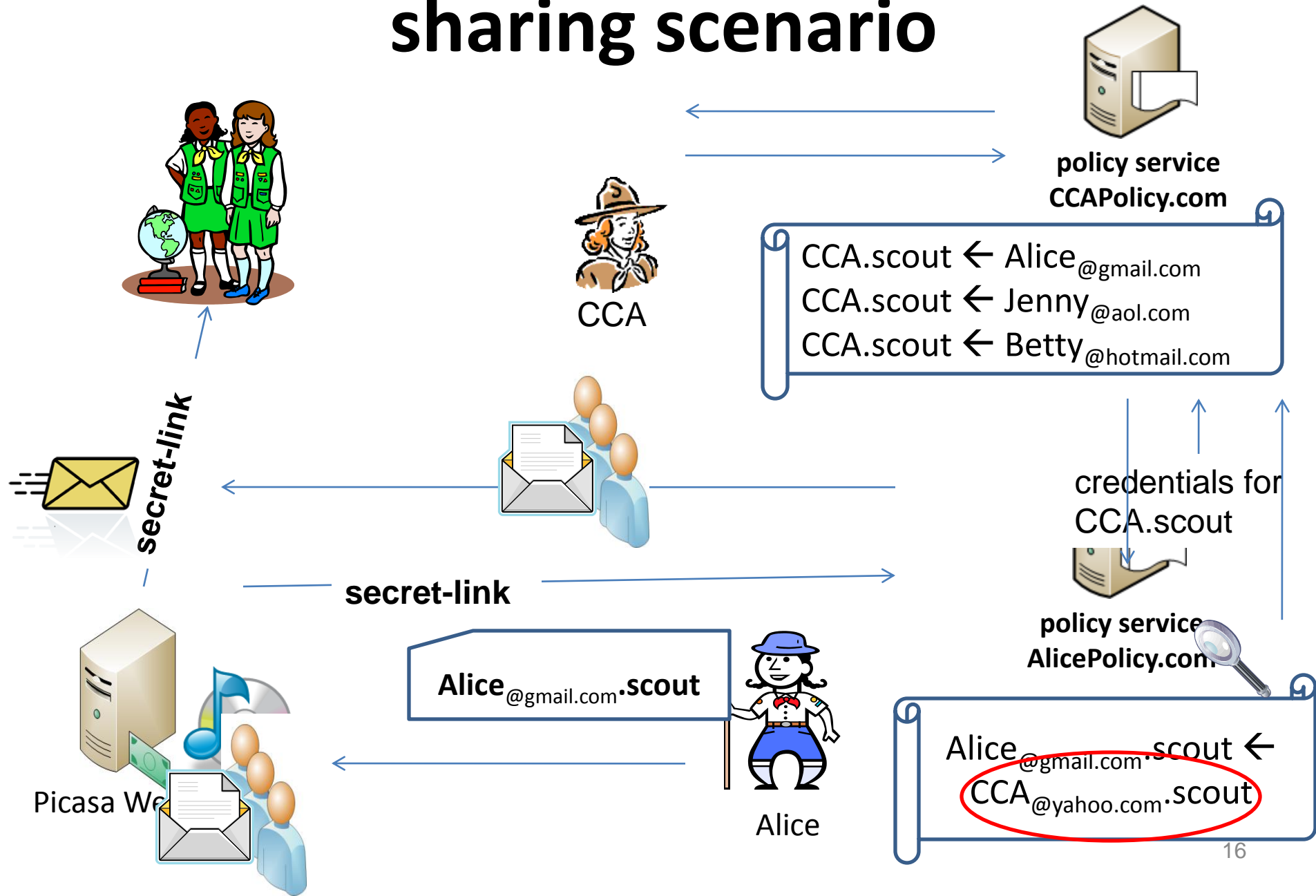
extends contact-lists to enable trust-
based access control

OpenID_{email} provider

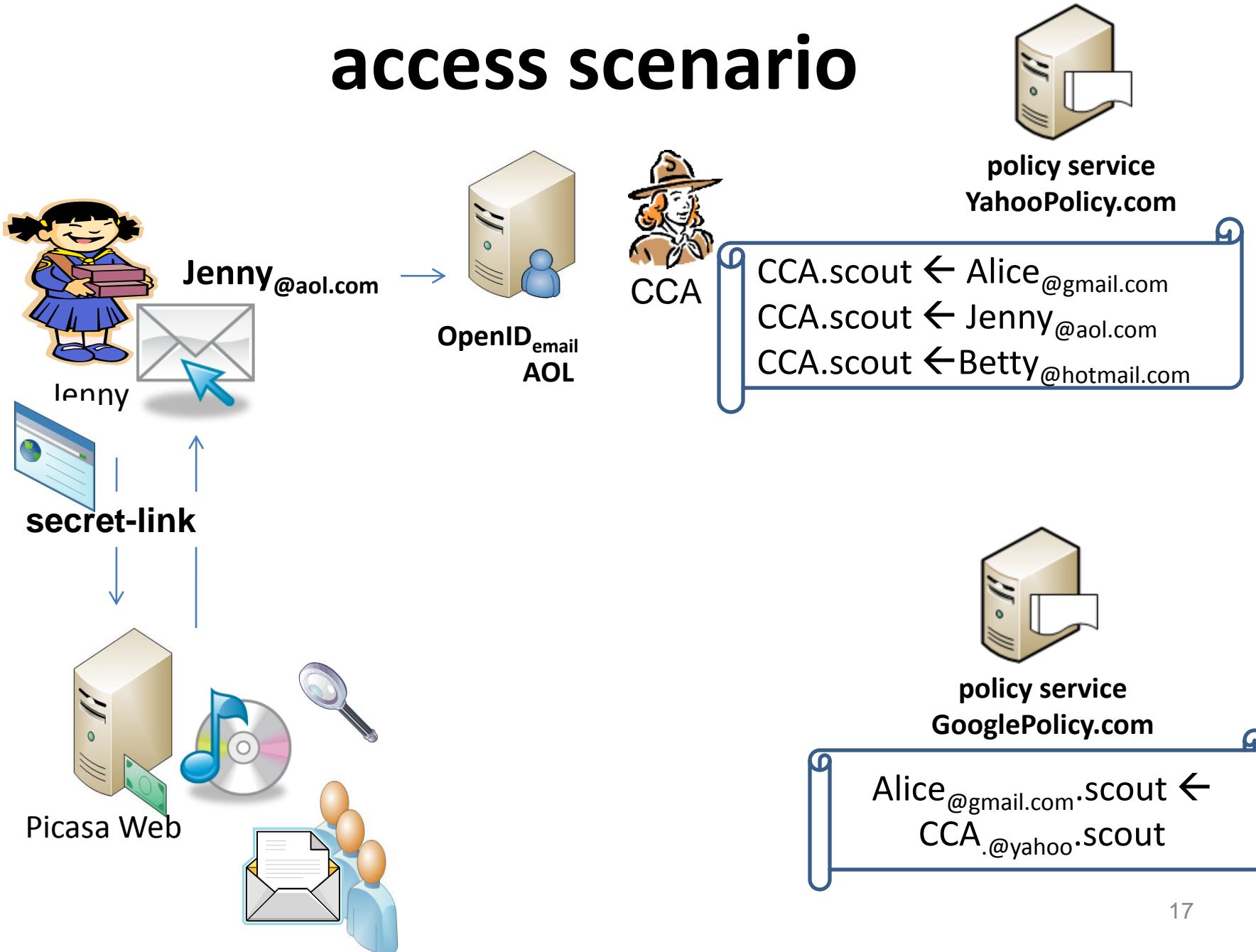
OpenPolicy provider

RT policy language

sharing scenario



access scenario

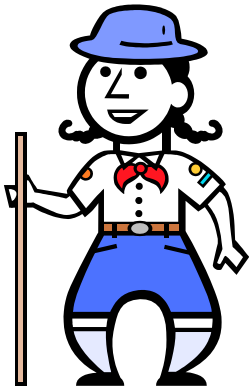


more complex sharing scenario



CCA scouts and their parents only

Canadian Coast Adventures (CCA)
Girl Scouts



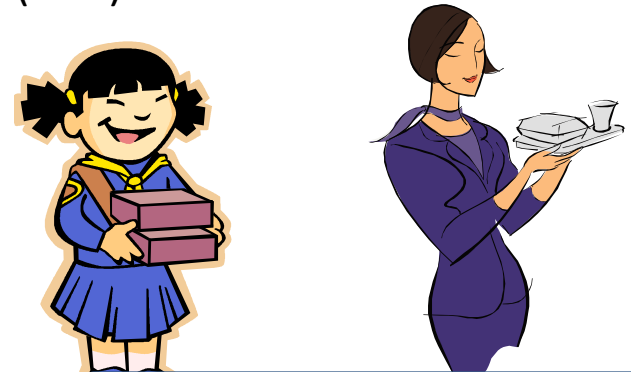
Alice



Picasa Web



Alice's scout friends in Picasa Web



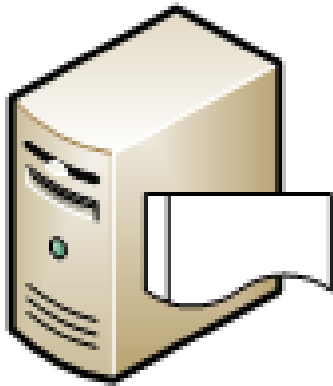
Jenny@aol.com·parent ←
Mary@hotmail.com

CCA.scout ← Jenny@aol.com

outline

- overview
- approach
- **implementation**
- conclusion

implementation

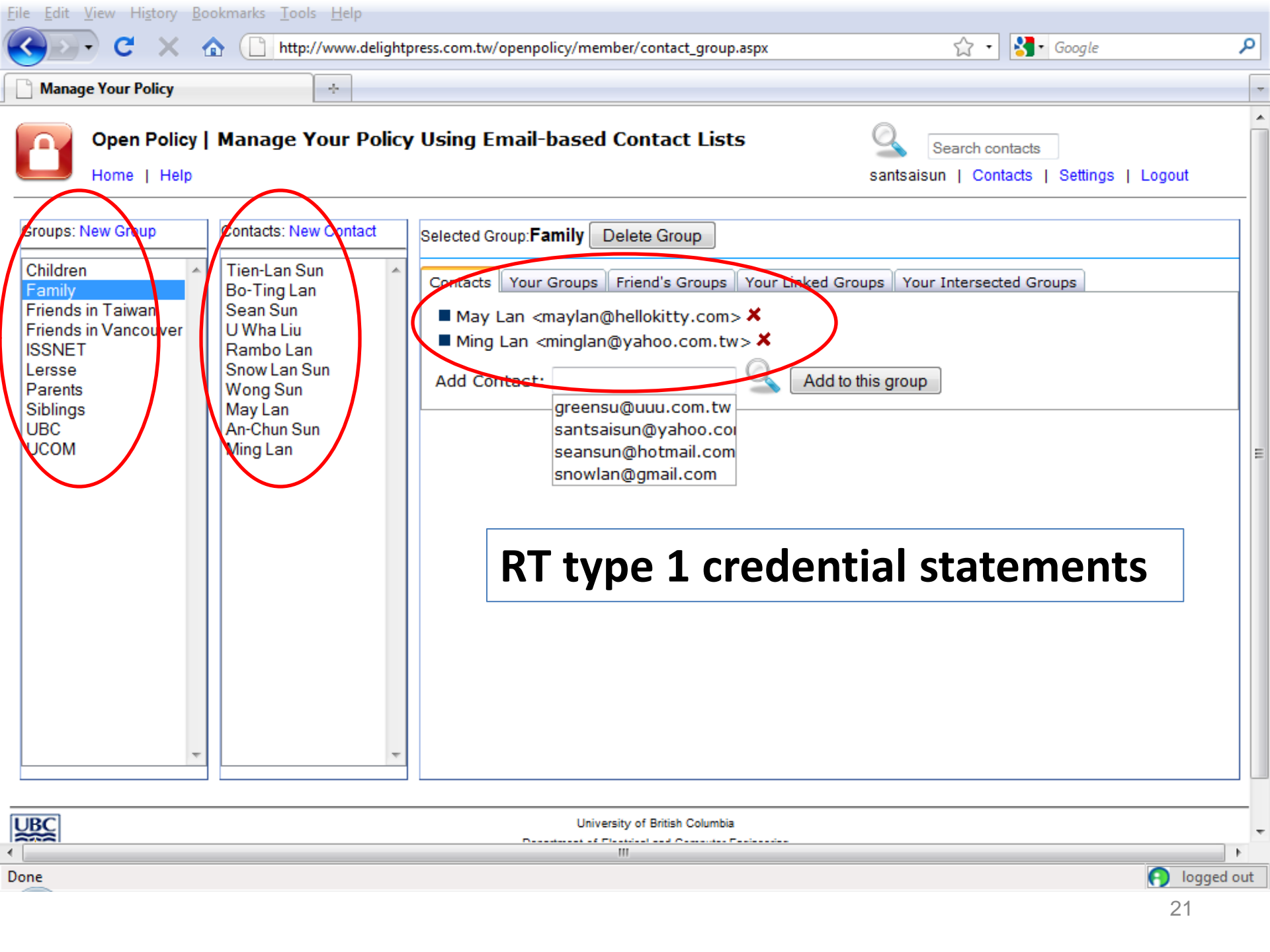


OpenPolicy



OpenID_{email}





Open Policy | Manage Your Policy Using Email-based Contact Lists

[Home](#) | [Help](#)

santsaisun | [Contacts](#) | [Settings](#) | [Logout](#)

- Groups: [New Group](#)
- Children
 - Family**
 - Friends in Taiwan
 - Friends in Vancouver
 - ISSNET
 - Lesse
 - Parents
 - Siblings
 - UBC
 - UCOM

- Contacts: [New Contact](#)
- Tien-Lan Sun
 - Bo-Ting Lan
 - Sean Sun
 - U Wha Liu
 - Rambo Lan
 - Snow Lan Sun
 - Wong Sun
 - May Lan
 - An-Chun Sun
 - Ming Lan

Selected Group: **Family** [Delete Group](#)

[Contacts](#) | [Your Groups](#) | [Friend's Groups](#) | [Your Linked Groups](#) | [Your Intersected Groups](#)

- May Lan <maylan@hellokitty.com> ✖
- Ming Lan <minglan@yahoo.com.tw> ✖

Add Contact: [Add to this group](#)

- greensu@uuu.com.tw
- santsaisun@yahoo.com
- seansun@hotmail.com
- snowlan@gmail.com

RT type 1 credential statements

Manage Your Policy

Open Policy | Manage Your Policy Using Email-based Contact Lists

Search contacts
santsaisun | [Contacts](#) | [Settings](#) | [Logout](#)

[Home](#) | [Help](#)

- Groups: [New Group](#)
- Children
 - Family**
 - Friends in Taiwan
 - Friends in Vancouver
 - ISSNET
 - Lesse
 - Parents
 - Siblings
 - UBC
 - UCOM

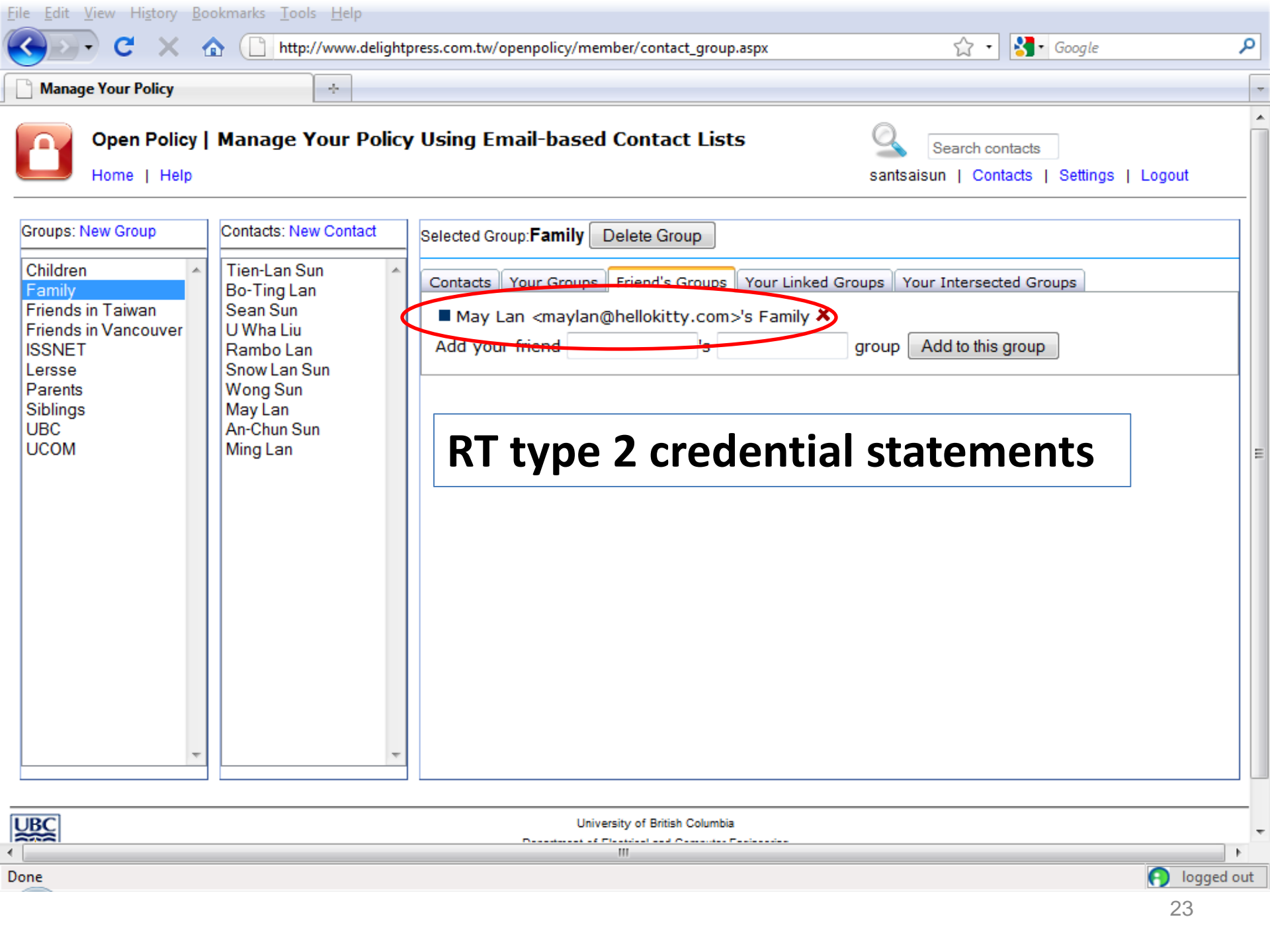
- Contacts: [New Contact](#)
- Tien-Lan Sun
 - Bo-Ting Lan
 - Sean Sun
 - U Wha Liu
 - Rambo Lan
 - Snow Lan Sun
 - Wong Sun
 - May Lan
 - An-Chun Sun
 - Ming Lan

Selected Group: **Family** [Delete Group](#)

[Contacts](#) | **[Your Groups](#)** | [Friend's Groups](#) | [Your Linked Groups](#) | [Your Intersected Groups](#)

- Siblings ✕
- Parents ✕
- Children ✕

Add group: [Add to this group](#)



Open Policy | Manage Your Policy Using Email-based Contact Lists

[Home](#) | [Help](#)

- Groups: [New Group](#)
- Children
 - Family**
 - Friends in Taiwan
 - Friends in Vancouver
 - ISSNET
 - Lersse
 - Parents
 - Siblings
 - UBC
 - UCOM

- Contacts: [New Contact](#)
- Tien-Lan Sun
 - Bo-Ting Lan
 - Sean Sun
 - U Wha Liu
 - Rambo Lan
 - Snow Lan Sun
 - Wong Sun
 - May Lan
 - An-Chun Sun
 - Ming Lan

Selected Group: **Family** [Delete Group](#)

[Contacts](#) [Your Groups](#) [Friend's Groups](#) [Your Linked Groups](#) [Your Intersected Groups](#)

■ **May Lan <maylan@hellokitty.com>'s Family** ✕

Add your friend 's group [Add to this group](#)

RT type 2 credential statements

- Groups: [New Group](#)
- Children
 - Family**
 - Friends in Taiwan
 - Friends in Vancouver
 - ISSNET
 - Lesse
 - Parents
 - Siblings
 - UBC
 - UCOM

- Contacts: [New Contact](#)
- Tien-Lan Sun
 - Bo-Ting Lan
 - Sean Sun
 - U Wha Liu
 - Rambo Lan
 - Snow Lan Sun
 - Wong Sun
 - May Lan
 - An-Chun Sun
 - Ming Lan

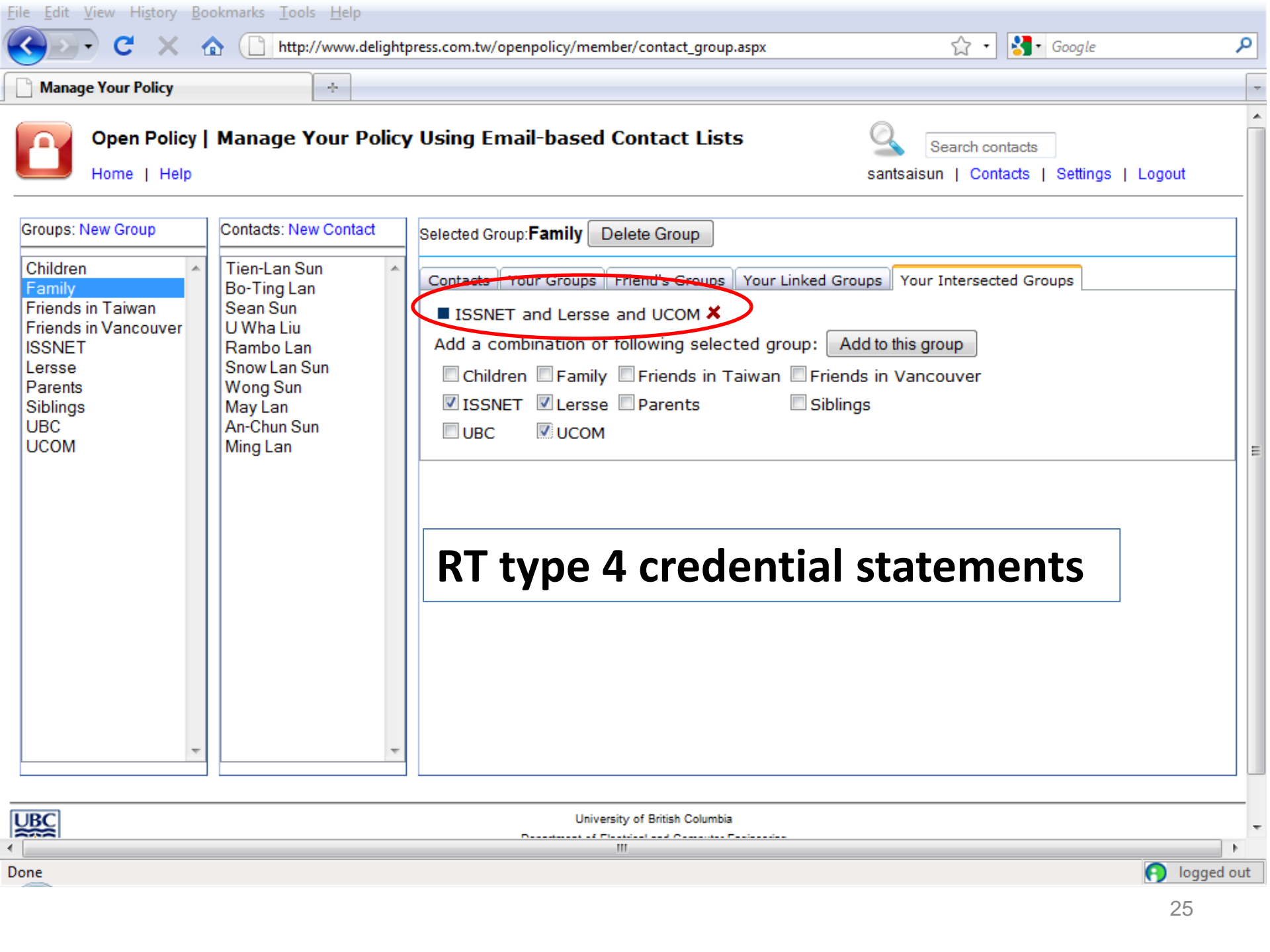
Selected Group: **Family** [Delete Group](#)

[Contacts](#) | [Your Groups](#) | [Friend's Groups](#) | [Your Linked Groups](#) | [Your Intersected Groups](#)

■ [Siblings]'s Family ✕

Add all members of your 's group [Add to this group](#)

RT type 3 credential statements



- Groups: [New Group](#)
- Children
 - Family**
 - Friends in Taiwan
 - Friends in Vancouver
 - ISSNET
 - Lersse
 - Parents
 - Siblings
 - UBC
 - UCOM

- Contacts: [New Contact](#)
- Tien-Lan Sun
 - Bo-Ting Lan
 - Sean Sun
 - U Wha Liu
 - Rambo Lan
 - Snow Lan Sun
 - Wong Sun
 - May Lan
 - An-Chun Sun
 - Ming Lan

Selected Group: **Family** [Delete Group](#)

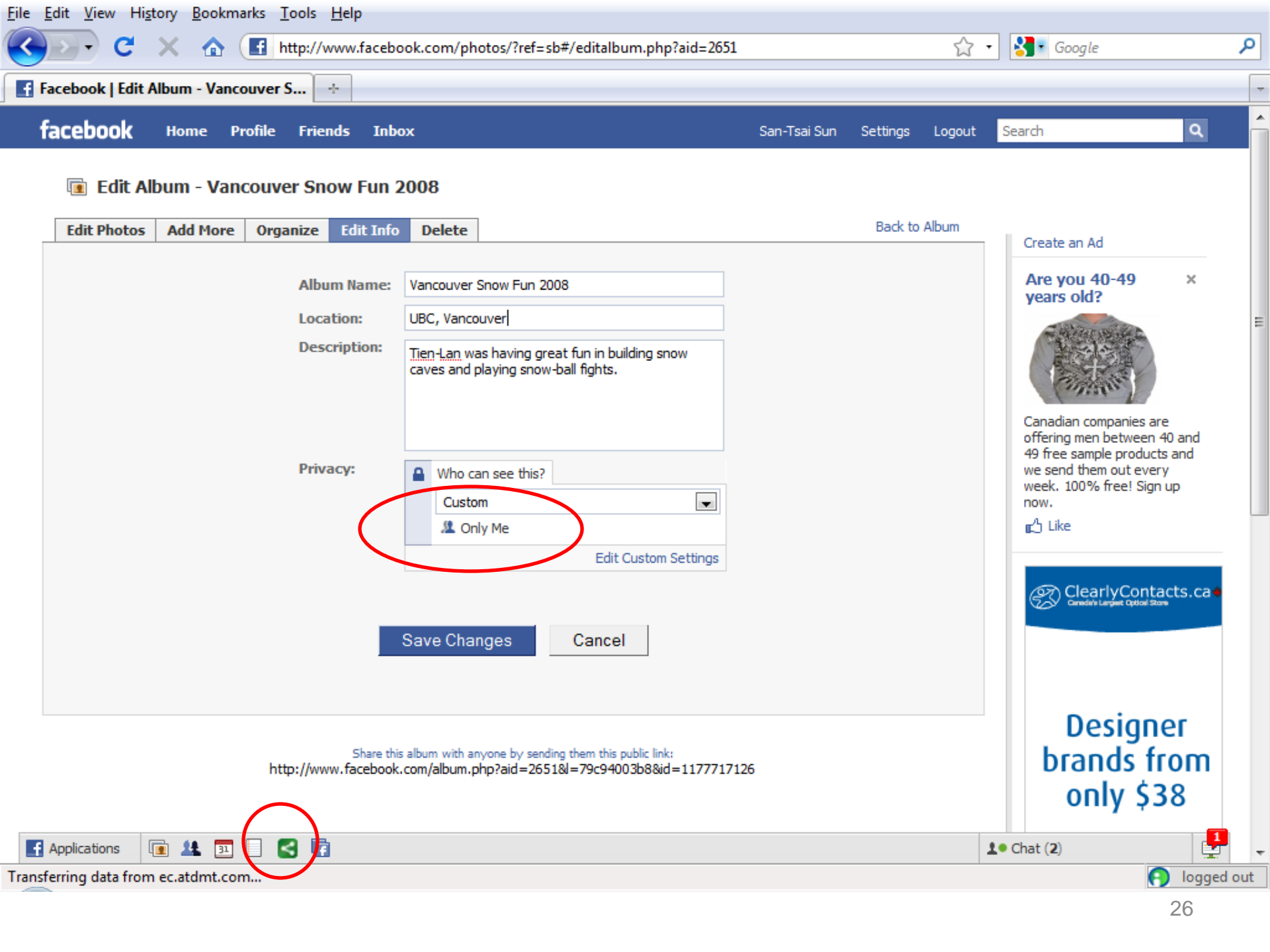
[Contacts](#) | [Your Groups](#) | [Friend's Groups](#) | [Your Linked Groups](#) | [Your Intersected Groups](#)

■ **ISSNET and Lersse and UCOM** ✘

Add a combination of following selected group: [Add to this group](#)

Children
 Family
 Friends in Taiwan
 Friends in Vancouver
 ISSNET
 Lersse
 Parents
 Siblings
 UBC
 UCOM

RT type 4 credential statements



Edit Album - Vancouver Snow Fun 2008

- Edit Photos
- Add More
- Organize
- Edit Info**
- Delete

[Back to Album](#)

Album Name: Vancouver Snow Fun 2008

Location: UBC, Vancouver

Description: Tien-Lan was having great fun in building snow caves and playing snow-ball fights.

Privacy: Who can see this?
Custom
Only Me
[Edit Custom Settings](#)

Save Changes

Cancel

Share this album with anyone by sending them this public link:
<http://www.facebook.com/album.php?aid=2651&l=79c94003b8&id=1177717126>

Create an Ad

Are you 40-49 years old?



Canadian companies are offering men between 40 and 49 free sample products and we send them out every week. 100% free! Sign up now.

Like

ClearlyContacts.ca
Canada's Largest Optical Store


Designer brands from only \$38




Share your albums with non-Facebook users


This is research project of LERSSE in the Department of Electrical and Computer Engineering at the University of British Columbia

 **Tien-Lan One-Year-Old** Share +
3 photos
Tien-Lan is one-year-old now.
Created 2009/11/24
Updated 2009/11/24

 **UBC Apple Festival** Share +
2 photos
The 19th annual Apple Festival, hosted by the Friends of the Garden, is being held on October 17th and 18th from 11 a.m. to 4 p.m. each day. A \$2.00 admission fee for adults helps support new garden initiatives -- for those under 12, admission is free.
Created 2009/11/24
Updated 2009/11/24

 **Vancouver Snow Fun 2008** Share +
8 photos
Tien-Lan was having great fun in building snow caves and playing snow-ball fights.
Created 2009/1/7
Updated 2009/11/24

Create an Ad

New Year's Eve 2010 ×

Start this year off right - party at the Commodore. Music by Famous Players and DJ Paul the Wall. Dinner and dance tickets for sale.
Like

Create an Ad on Facebook ×

Reach over 300 million active users on Facebook. Learn how to connect your business to real customers through Facebook Ads.
Like

Select Recipients of Secret-Link

Open Policy | Manage Your Policy Using Email-based Contact Lists

Home | Help

Select Recipients of Secret-Link

All Contact Groups

- Children
- Family
- Friends in Taiwan
- Friends in Vancouver
- ISSNET
- Lersse
- Parents
- Siblings
- UBC
- UCOM

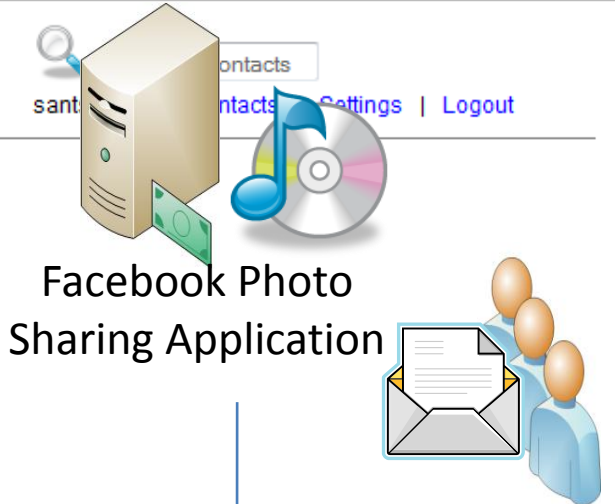
Target Groups

- Family
- Lersse

Selected Contacts

- Tien-Lan Sun
- Bo-Ting Lan
- Sean Sun
- U Wha Liu
- Rambo Lan
- Wong Sun
- May Lan
- An-Chun Sun
- Ming Lan
- Pranab Kini

Send



secret-link

The following link will be sent out to each member of the selected target groups:

Facebook Photo Sharing Application




Photo Album: **Vancouver Snow Fun 2008**
Description: Tien-Lan was having great fun in building snow caves and playing snow-ball fights.

San-Tsai has shared a link to an album with you. To view the album, follow this link:
<http://apps.facebook.com/fbshares/access.aspx?s=5058256540109113947>

San-Tsai Sun
2009-12-03 04:21:05





Search: Web Search

Epson Artisan® 810
A BRILLIANT gift for the whole family
Save \$70 now
WiFi Ethernet

Mail | Contacts | Calendar | Notepad | What's New? - Mobile Mail - Options

Check Mail | New | Mail Search | Try the new Yahoo! Mail

Chat with your pals in Yahoo! Mail

- Folders [Add]
- Inbox (14)
- Drafts
- Sent
- Spam [Empty]
- Trash [Empty]
- My Photos
- My Attachments

Chat & Mobile Text [Hide]
I am Available
0 Online Contacts [Add]

Previous | Next | Back to Messages | Mark as Unread | Print

Delete | Reply | Forward | Spam | Move...

Facebook Photo Album Sharing Tuesday, November 24, 2009 6:22 AM

From: "service@delightpress.com.tw" <service@delightpress.com.tw>
To: santsaisun@yahoo.com

Facebook Photo Sharing Application

Photo Album: **Vancouver Snow Fun 2008**
Description: Tien-Lan was having great fun in building snow caves and playing snow-ball fights. San-Tsai has shared a link to the above album with you. To view the album, follow this link:
<http://apps.facebook.com/fbshares/access.aspx?s=5058256540109113947>

San-Tsai Sun
2009-11-24 10:19:05

Delete | Reply | Forward | Spam | Move...

Previous | Next | Back to Messages | Select Message Encoding | Full Headers

facebook

Keep me logged in

[Forgot your password?](#)

Login

Sign Up

Sign up for Facebook to use Sharing beyond walled garden.

You do not need to sign up Facebook, just login using your existing email account.






fbshares.rpxnow.com

Sign in to fbshares.rpxnow.com with your Yahoo! ID

Sign in to Yahoo!

 **Are you protected?**
Create your sign-in seal.
(Why?)

Yahoo! ID:

(e.g. free2rhyme@yahoo.com)

Password:



Sign In

[I can't access my account](#)

facebook

Keep me logged in

[Forgot your password?](#)

Email

Password

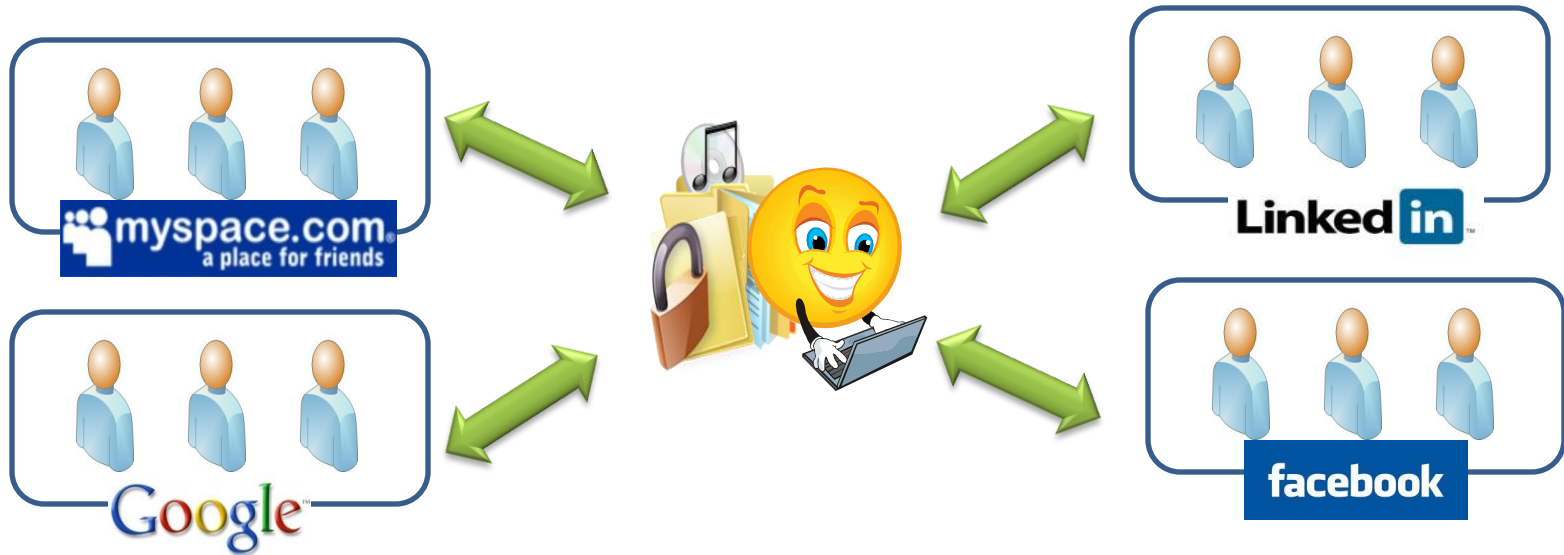
Login

Sign Up

Sign up for Facebook to use Sharing beyond walled garden.



conclusion



Web-based content sharing mechanism



conclusion

- our solution is user-centric
 - Web users use the same identity and access policy across CSPs, and they are free to choose them
- only use browser, sharing experiences are similar to users' existing file/content practices
 - email, secret-link
- CSPs are not required to change their existing access-control mechanism
 - integrate their secret-link mechanism with OpenPolicy and OpenID_{email} provider

extend OpenID

- OpenID relies on redirection during authentication
 - vulnerable to phishing attacks
- build OpenID support into browser
 - function without redirection

□ San-Tsai Sun and Konstantin Beznosov. “Poster: OpenID_{email} Enabled Browser,” in ACSAC 2009 poster session, Honolulu, Hawaii, USA . Dec. 9th 2009.

□ San-Tsai Sun, Kirstie Hawkey, and Konstantin Beznosov. “Web Single Sign-On with OpenID_{email} Enabled Browser”. Under review.

enhance trust-management

- detect who is abusing the trust of others
 - Jenny could allow her friend Bob to view CCA's photos
- control the depth of transitive trust
 - $A \text{ trusts } B \cap B \text{ trusts } C \rightarrow A \text{ trusts } C$

usability evaluation

- heuristic evaluation
- cognitive walk-through
- lab experiment



questions?

Secure Web 2.0 Content Sharing Beyond Walled Gardens

san-tsai sun <santsais@ece.ubc.ca>

Department of Electrical and Computer Engineering
Laboratory for Education and Research in Secure Systems Engineering (**LERSSE**)

sharing scenario 1



secret-link



policy service
YourPolicy.com

secret-link,
Alice@gmail.com.scout

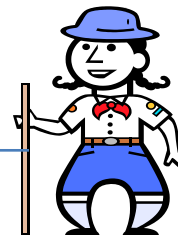


Picasa Web



Alice@gmail.com.scout

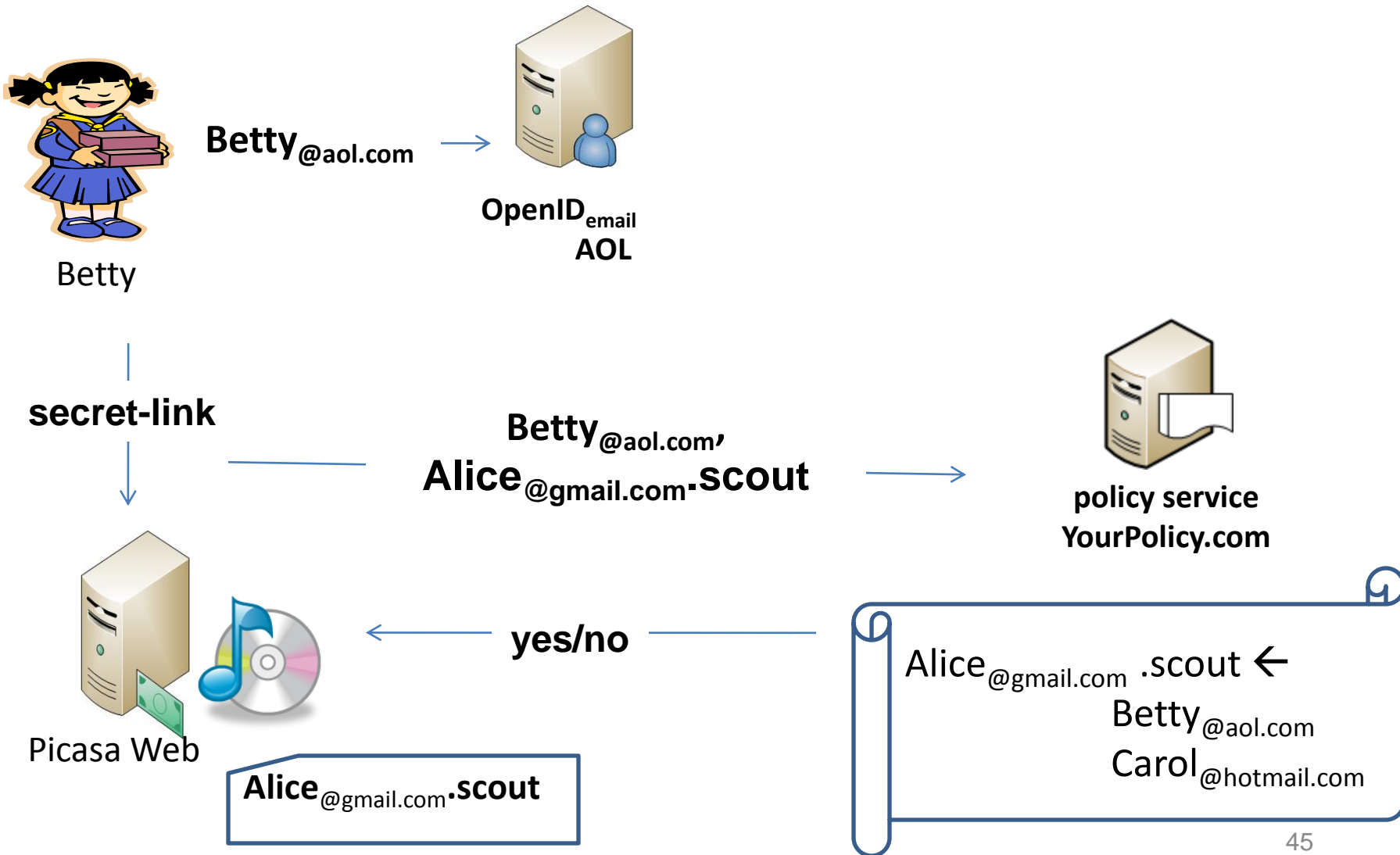
Alice@gmail.com.scout



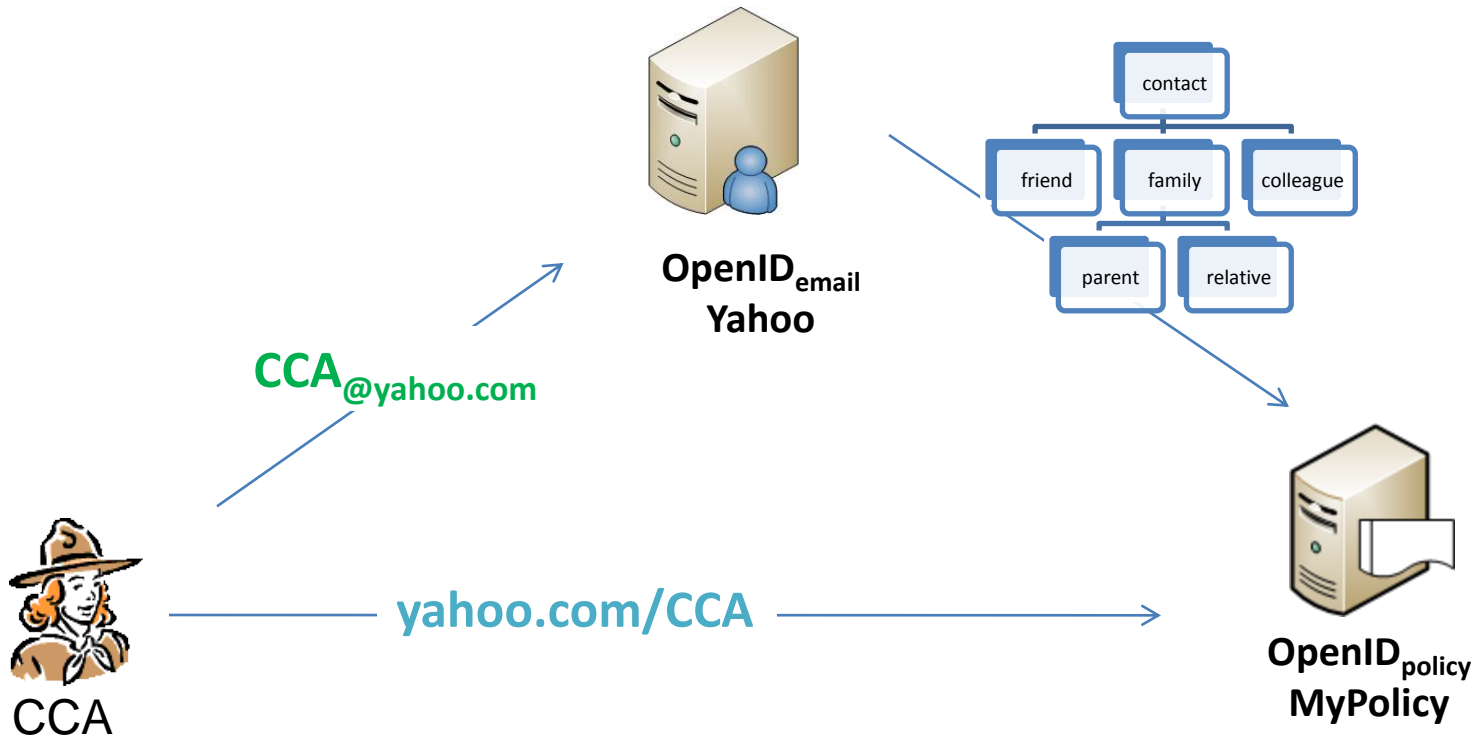
Alice

Alice@gmail.com .scout ←
Betty@aol.com
Carol@hotmail.com

access scenario 1

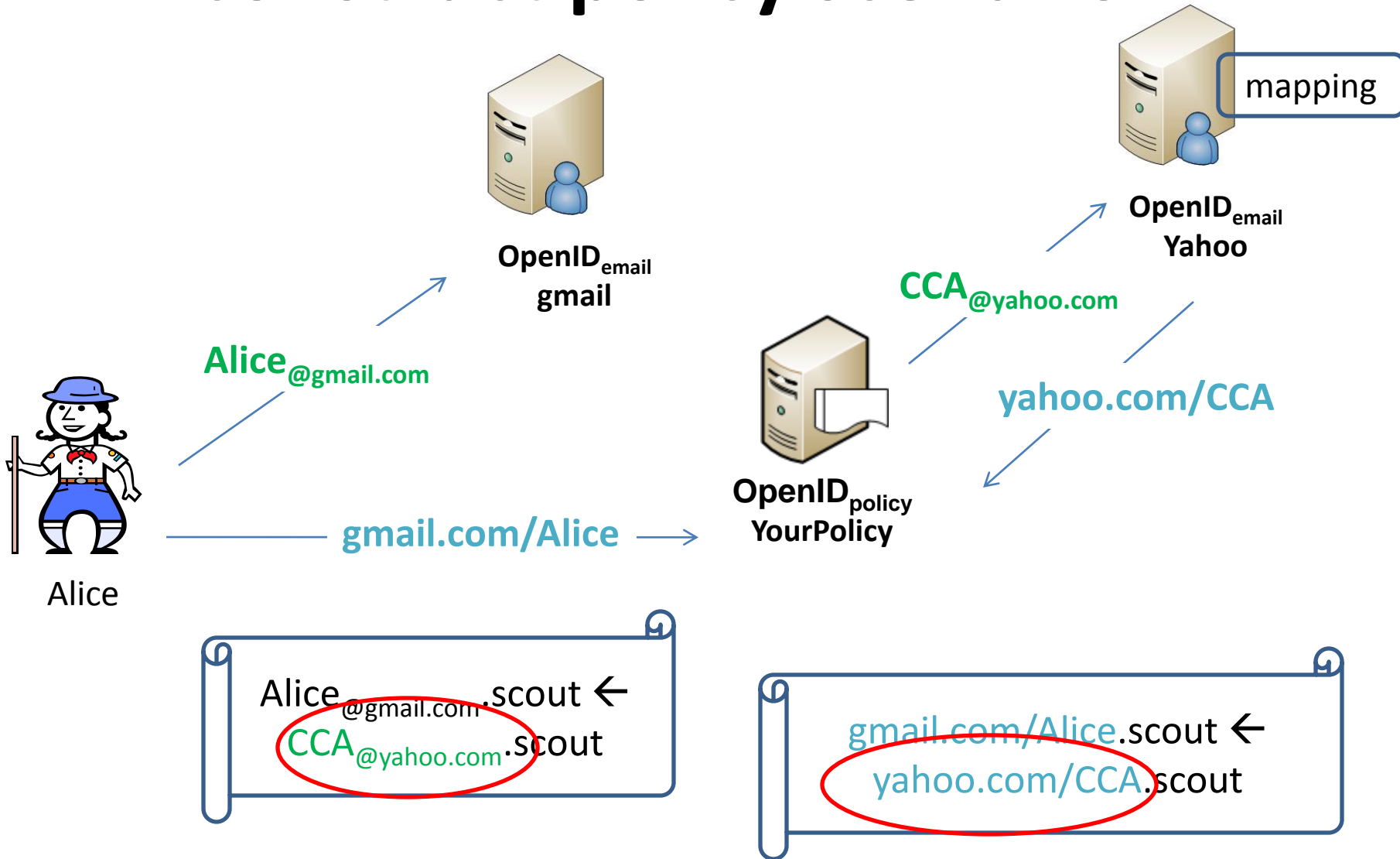


policy import scenario



CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com

construct policy scenario



sharing scenario (detail)



policy service
MyPolicy



CCA

CCA.scout ← Alice@gmail.com
CCA.scout ← Jenny@aol.com
CCA.scout ← Betty@hotmail.com

secret-link,
yahoo.com/jenny ...

OpenID_{email}
Yahoo

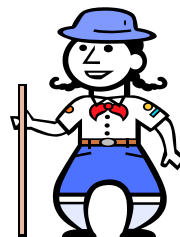
credentials

CCA.scout ←
aol.com/jenny

secret-link,
gmail.com/Alice.scout

policy service
YourPolicy

Alice@gmail.com.scout ←
CCA@yahoo.scout



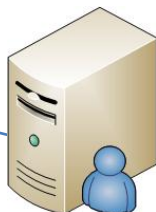
Alice

gmail.com/Alice.scout

gmail.com/Alice.scout



OpenID_{email}
gmail



secret-link,
gmail.com/Alice.scout



policy service
YourPolicy

Alice@gmail.com.scout ←
CCA@yahoo.scout



Picasa Web



gmail.com/Alice.scout

gmail.com/Alice.scout

gmail.com/Alice
yourPolicy

access scenario

