



EIFL
Thursday, December 15th, 2011

Brook Schofield
Project Development Officer
brook@terena.org
www.terena.org

Building Federated Identity Infrastructure



Building an Identity Federation

- › Chicken & Egg
 - › Identity Providers with People
 - › Service Providers with Resources

- › How can I be an identity provider?
 - › Do you have information on people?
 - › Choose some software...
 - › Success!

- › What about service providers?
 - › EIFL talks to publishers
 - › There are other resources available too...

- › Why do federated identity at all?





How big is your problem?

- › How many “login” boxes do you have in your campus?
 - › If it is more than one – you need federated identity.
 - › Use Google to search
 - › site:auca.kg login
 - › site:your.domain sign-in
 - › site:your.domain.org password
- › Then make a spreadsheet...

	A	B	C	D	E	F
1	Site	URL	Product	Audience	Authentication	Importance
2	Course management	http://e-course.auca.kg/	Moodle	Staff/Students	Windows Username/Password	High
3	e-Portfolio system	http://eportfolio.auca.kg/	Mahara	Staff/Students	Windows Username/Password	Moderate
4	Alumni system	http://eportfolio.auca.kg/alumni.php	?	Alumni	Separate System	Low
5	Library Remote Access	http://library.auca.kg/en/remote_access/	Ezproxy	Library Users		
6	Library Databases	http://library.auca.kg/en/databases/	Off-site		IP Auth (no off campus access)	
7	Library Patron System	http://library.auca.kg/en/authentication/	Follet	Library Users	Self Sign Up	
8	Forum system	http://forum.auca.kg/	InvisionPower	Uni Community		
9	Webmail	http://mail.auca.kg/	Roundcube	Staff/Students		
10	Apply Online	http://applyonline.auca.kg/		Potential Students		
11	Career Application	http://career.auca.kg/		Students		



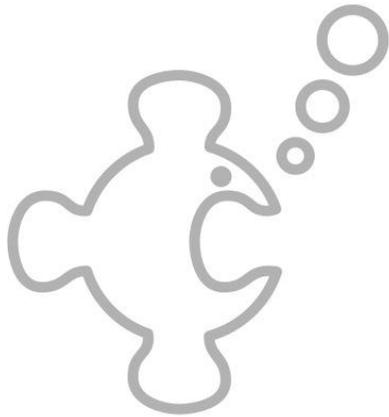
Skills required...

- › Concentrate on the skills you have or those you want to develop.



Shibboleth[®]

- › Separate IdP/SP/DS
- › IdP is Java (runs within Tomcat)
- › SP is C (supports Apache + IIS)

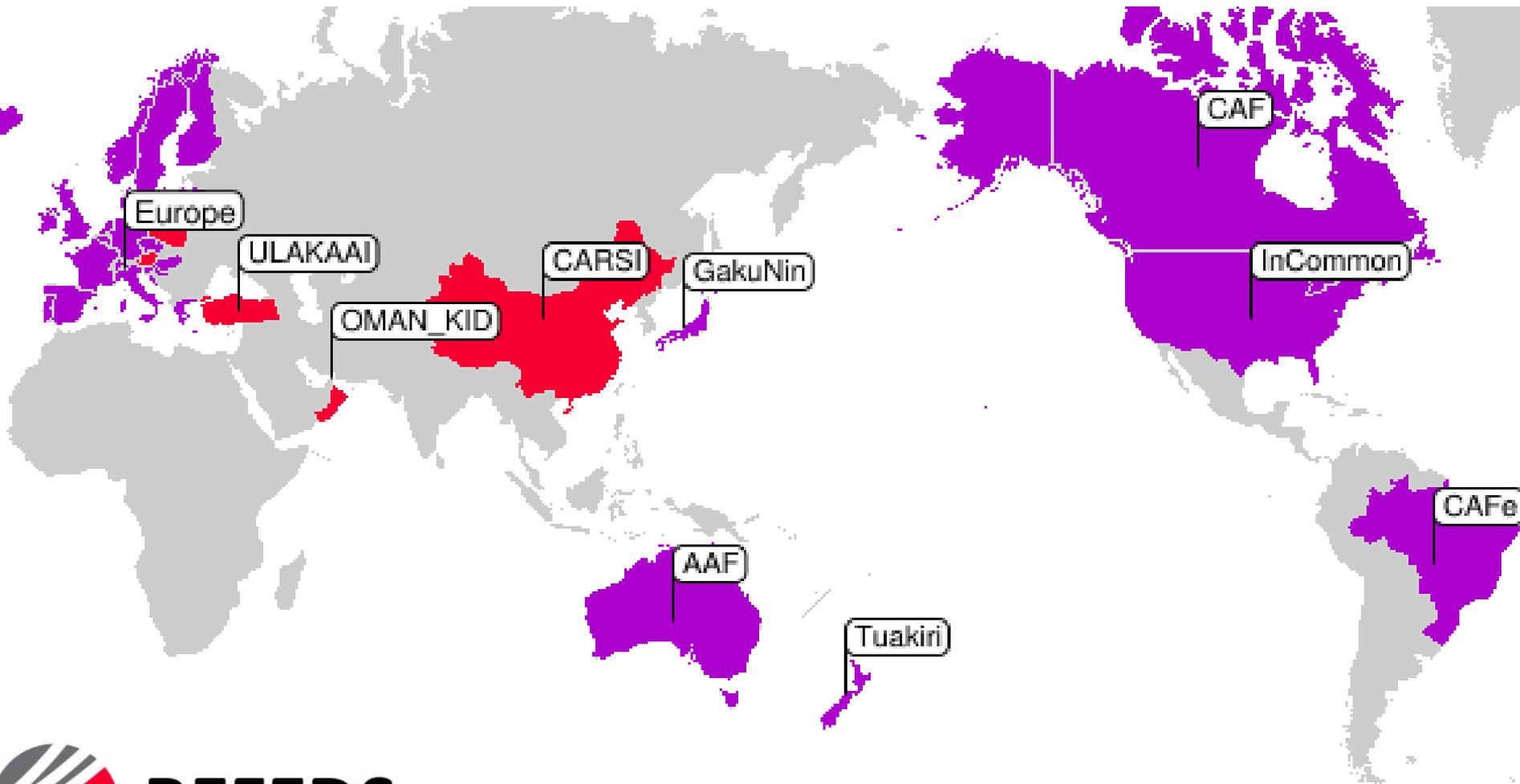


- › simpleSAMLphp from UNINETT
 - › Integrated IdP/SP/Bridge/Disco
 - › SAML 2.0/OAuth/OpenID
 - › Facebook, Google, Windows Live
 - › PHP (AUCA run their IdP on Microsoft Windows)
 - › Multi-lingual interface (includes support for RTL languages).



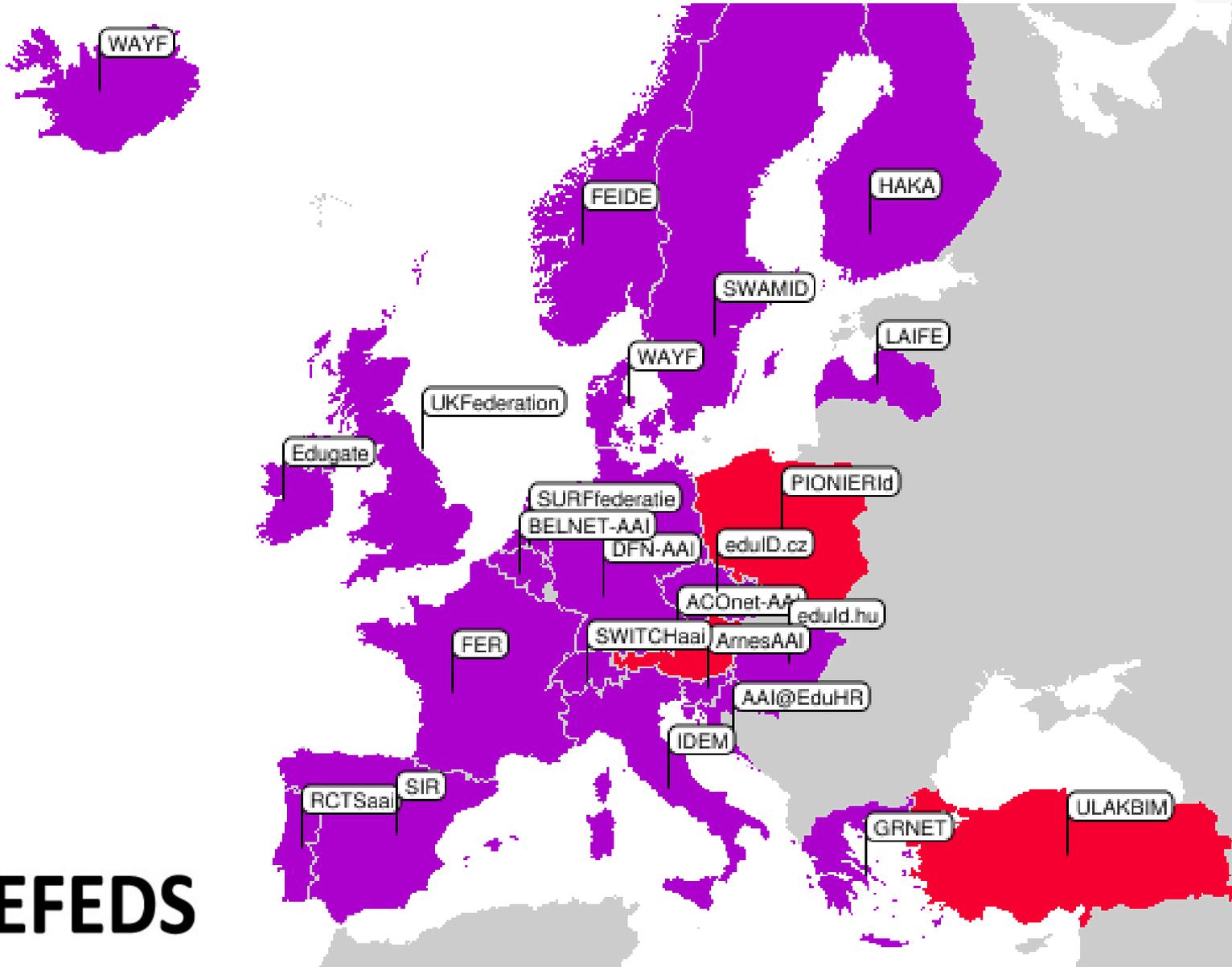
Where are Identity Federations?

■ Pilot ■ Production





European Identity Federations





Federations you're NOT a part of...



AUSTRALIAN
ACCESS FEDERATION



DFN-AAI



cafe

edu



cz



SIR



haka

Edu gate

Gaining Access
to Education



SWITCH
aai



idem
garr aai

SURF

FEDERATIE

WAYF

Where are you from



Carisi



GakuNin

FEIDE

InCommon®



Tuakiri
NEW ZEALAND ACCESS FEDERATION



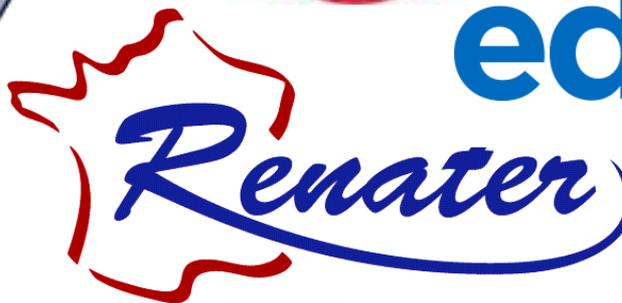
@ Edu Hr

edu ID



swami

RCTS aai
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

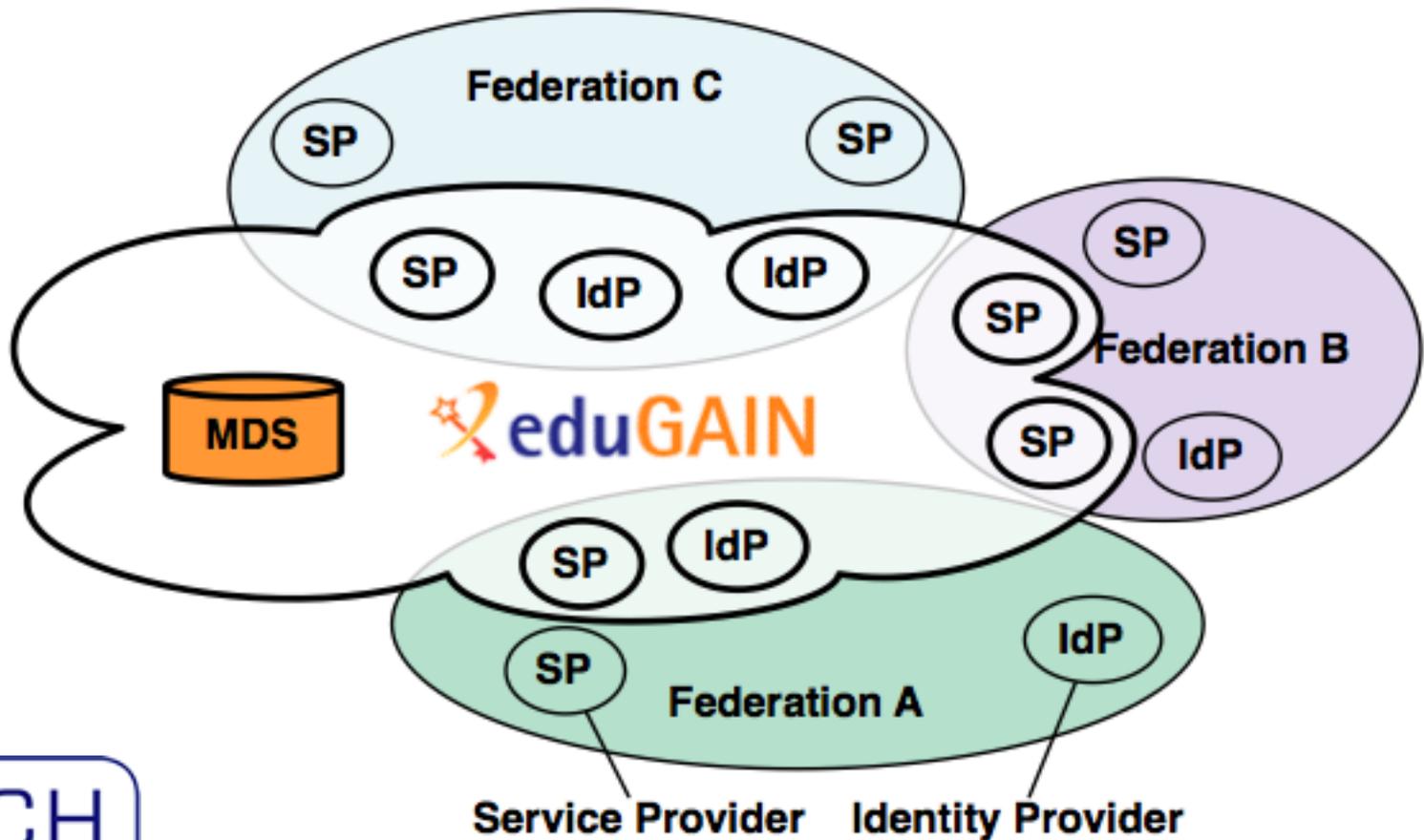


confia



How do I connect to everyone?

- › eduGAIN solves the scaling problem for Services
- › No longer join “customers” federation but instead join your “preferred” federation.





What should I do next?

- › Download the EuroCAMP Materials 
 - › Sign-up for a Dynamic DNS account (free)
 - › Run through the training
 - › Provide me with feedback - is it confusing?
- › Deploy a Campus Identity Federation
 - › AUCA didn't have the above materials!
 - › AMRES is scaling the service for Serbia.
- › Tell publishers/EIFL that this is what you want!
- › Technology is only part of the solution
 - › Policy is important too!
 - › Technology can work on your campus now and build a valuable service to justify future policy effort.



EuroCAMP Istanbul



- › Building Federated Identity Infrastructure 3-Day Event
 - › simpleSAMLphp IdP
 - › Shibboleth SP
 - › JANUS for Metadata Management
- › 19 Participants / 9 countries
 - › Armenia
 - › Azerbaijan
 - › Belarus
 - › Estonia
 - › Lithuania
 - › Moldova
 - › FYR Macedonia
 - › Serbia
 - › Turkey



EuroCAMP Amsterdam

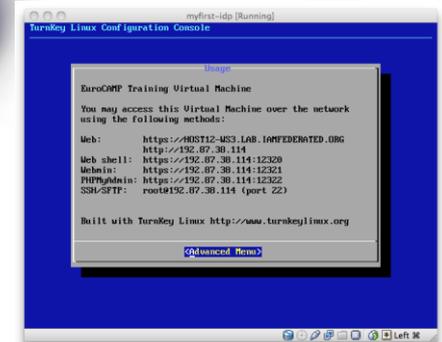


- › Building Federated Identity Infrastructure 3-Day Event
 - › simpleSAMLphp IdP
 - › Shibboleth SP
 - › JANUS for Metadata Management
- › 19 Participants/10 countries
 - › Bulgaria
 - › Cyprus
 - › Estonia
 - › Georgia
 - › Israel
 - › Latvia
 - › Lithuania
 - › Romania
 - › Russia
 - › Slovakia



What's in the course materials?

- › Virtual Machine Player
 - › VirtualBox or equivalent
- › Virtual Machine Image
 - › Based on TurnKey LAMP
 - › Preinstalled Apache, SSL Certificates, simpleSAMLphp, Shibboleth, MySQL, LDAP, DynamicDNS
- › Training Materials
 - › Intro to Federated Identity (activity)
 - › Setup your environment (hands on VM)
 - › My First IdP (hands on and information)
 - › Shibboleth Service Provider (hands on)
 - › JANUS for Metadata Management

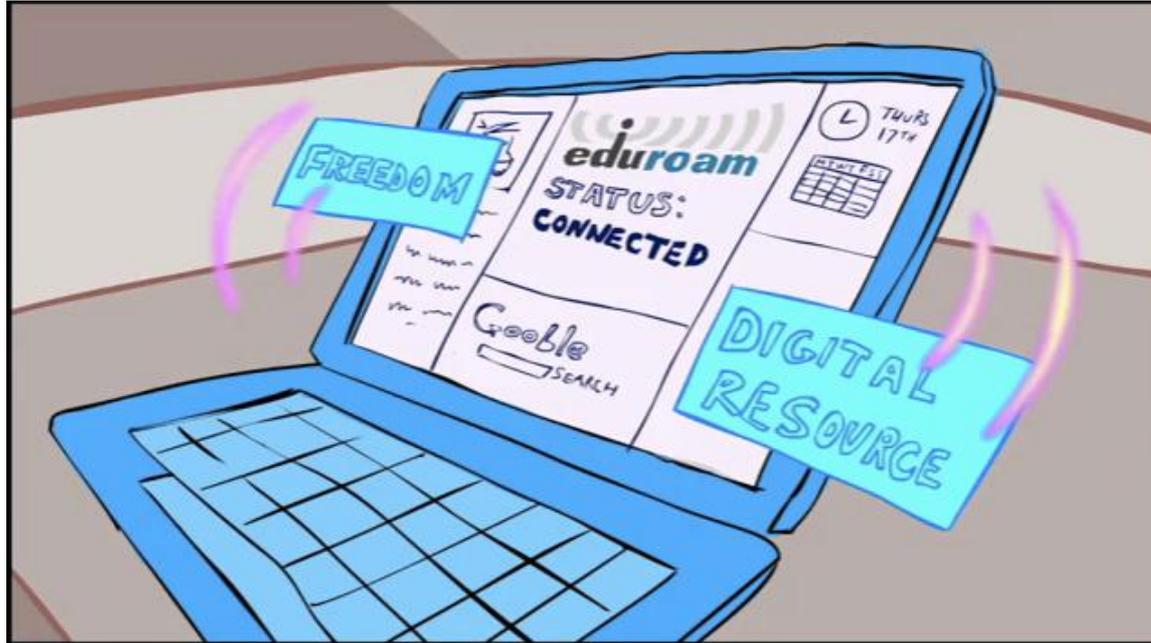


Shibboleth®





eduroam



« networking the networkers »



linkedin.com/in/brookschofield
facebook.com/brook.schofield
skype://brookschofield
brook@terena.org
@BrookSchofield
+31651553991



Questions?

**"Give a Man a Fish, Feed Him For a Day.
Teach a Man to Fish, Feed Him For a Lifetime"
Lao Tzu**