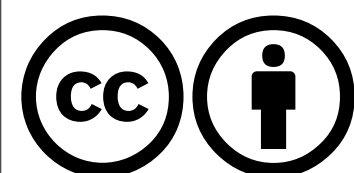


tigr: a novel take on two-factor authentication


LISA 2011, Boston, MA



Roland van Rijswijk
roland.vanrijswijk@surfnet.nl



Overview

- Introduction
- The 2-factor landscape
- Something we all have
-  **tiqr**
- Comparison of 2-factor AuthN technologies
- Security audit
- Questions?

Recognize this?

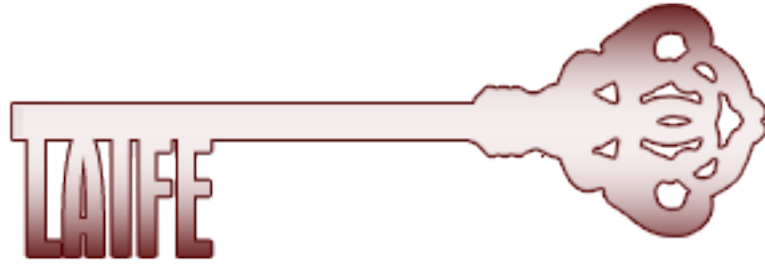
The image is a collage of various login and authentication interfaces. At the top left, there's a 'Welcome to SUGARCOMMUNITY EDITION' form with fields for 'User Name' (containing 'rijswijk') and 'Password', and a 'Log In' button. To its right is a 'sign in' form for 'Windows Live ID' with fields for 'Windows Live ID' and 'Password', and a 'Sign in' button. Further right is an 'Inloggen met Identifier' form with fields for 'Gebruikersnaam' and 'Wachtwoord', and an 'Inloggen' button. Below these are several other forms: a 'Sign in with your Google Account' form with 'Email' and 'Password' fields; a 'Novell. Nsure SecureLogin' dialog box with 'Username', 'Password', and 'Other field' fields; a 'SomeApplication' dialog box with 'User name' and 'Password' fields; and a 'vmware' login form with 'Username', 'Password', and 'Version' fields. There are also various other login forms and buttons scattered throughout, such as 'Inloggen met gebruikersnaam en w...', 'Uw gebruikersnaam of wachtwoord vergeten?', and 'Log In' buttons on different backgrounds.

United Federation of Passwords



WAYF

Where are you from



SURF

FEDERATIE



OpenID



haka

RCTS aai

InCommon
FEDERATION



SIR

AAI @ Edu Hr

edu ID cz

SWITCH
aai

The UK
Access
Management
Federation

FOR EDUCATION AND RESEARCH



FEIDE



cafe comunidade
acadêmica federada

eduID



KALMAR2



Tuakiri

New Zealand
Access Federation

Edu gate
Gaining Access
to Education

Well-known drawbacks

- The woes of usernames/passwords are well known... **Does anybody remember these guys?**



 **Study Reveals 75 Percent of Individuals Use Same Password for Social Networking and Email**

By SecurityWeek News on Aug 16, 2010

[Twitter](#)

FORGOTTEN PASSWORD

Forgotten Password

Please enter your email address below. A new password will be issued and sent to you.

E-mail Address:

Please [contact us](#) if you have any question.

PM's office passwords pose security risk

More than 10 per cent of passwords used in the Prime Minister's department can be easily broken in an hour by hackers

AAP (AAP) | 29 March, 2011 14:01 | [Comments](#) | [Like](#)

Endless patches and 'solutions'

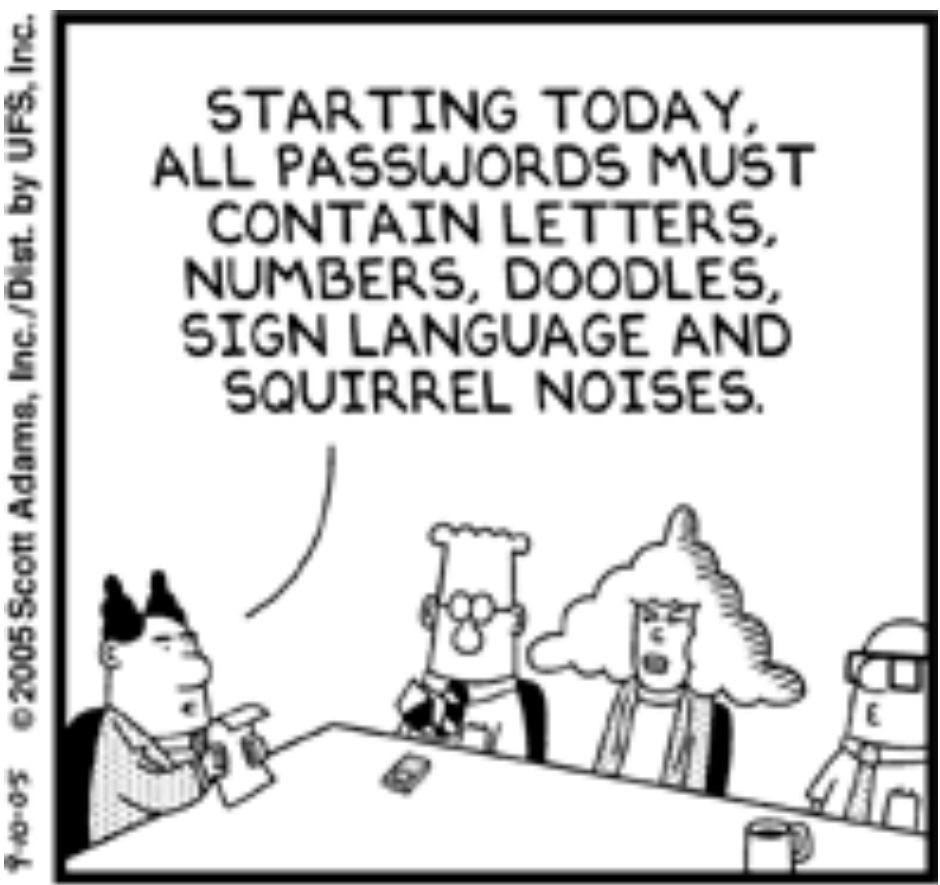
Change Expired Password

Your password must contain a number, an upper and lower case character, and a special character. Passwords cannot contain more than 3 of the following properties: repeating characters, incremented or decremented numeric or alphabetic strings. Please try again.

Current Password:

New Password:

Re-Enter New Password:



Change Password

Microsoft Windows Server 2003 Standard Edition

Copyright © 1985-2003 Microsoft Corporation

Passwords used on this network must comply with the rules set out below. If your new password does not comply with all these rules, the system will reject it and you will need to choose a different password.

Your new password must:

- not be the same as your previous 24 passwords
- not be similar to your logon name
- not be similar to your name
- not be similar to other commonly used passwords
- contain at least 3 of the following character types:
 - upper alpha
 - lower alpha
 - numeric
 - special
- contain at least 8 characters

User name:

Log on to:



Account Security hide

To help keep your Facebook account as safe as possible, we can notify you when your account is accessed from a computer or mobile device that you haven't used before.

Would you like to receive notifications for logins from new devices?

Yes No

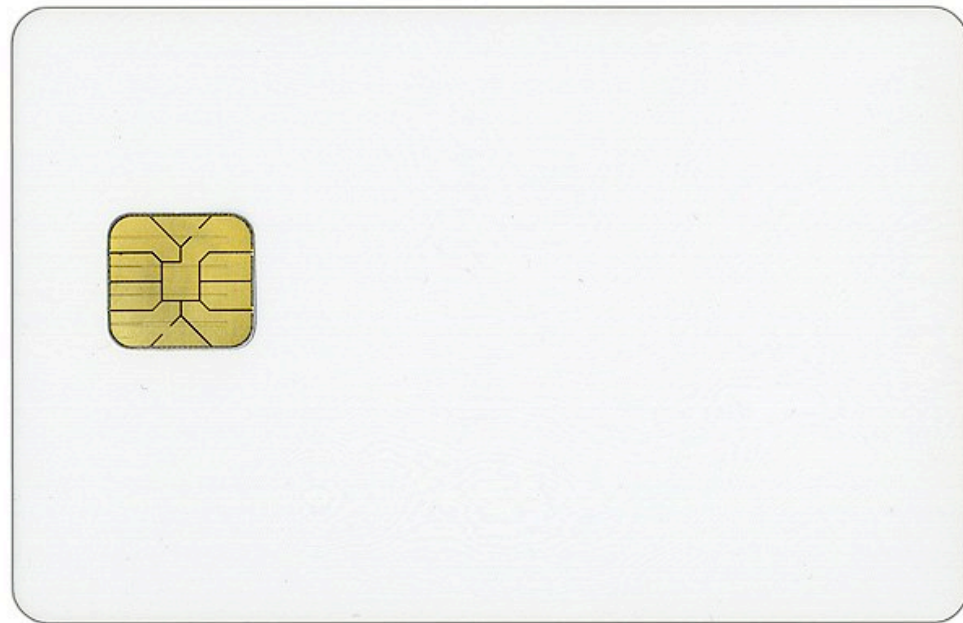
Notification methods (in addition to email):

SMS (mobile text)

Computers and mobile devices currently associated with your account:

Name	Time Saved	
Lev's Work Computer	Today at 1:00pm	Remove
Lev's Home Computer	Today at 12:59pm	Remove

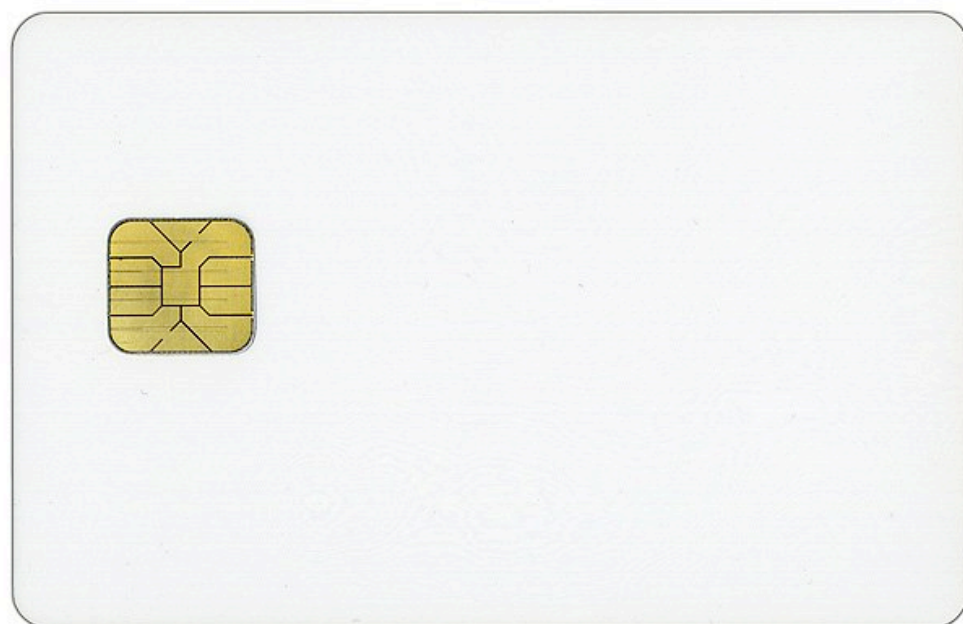
2-factor AuthN in one slide



+



=



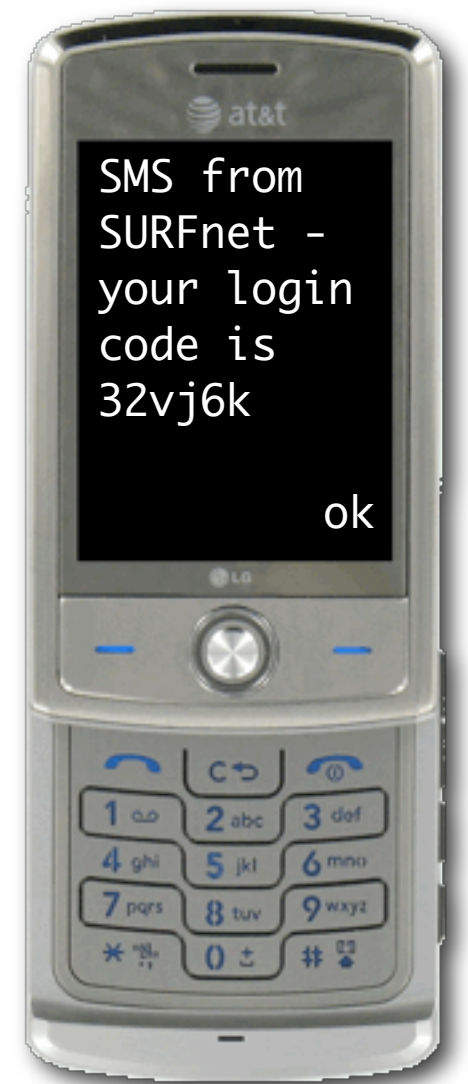
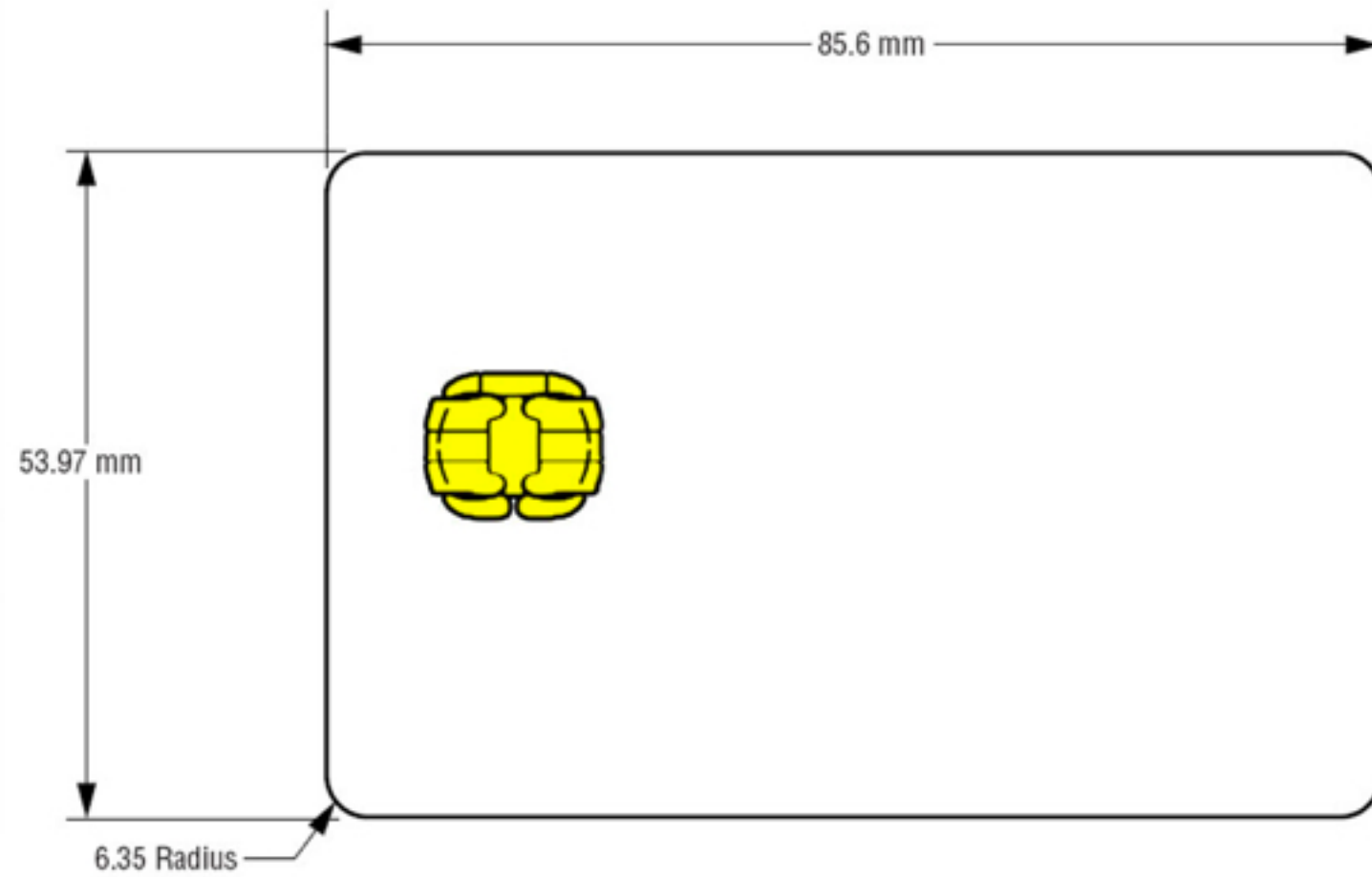
+



=



The 2-factor AuthN landscape



Drawbacks of 'traditional' 2-factor AuthN solutions

- Often involve additional physical tokens that users need to carry around
- May require driver software on end-user workstations
- Are proprietary in nature and incompatible with each other
- Are usually single purpose (e.g. you cannot use bank A's token for bank B as well)

Something we all have (right?)

- (Almost) everybody owns a mobile phone
 - A 2007 study in The Netherlands showed 19 million subscribers in a country with 16.5 million people
- Most people always carry their mobile phone with them
 - A recent study by SecurEnvoy shows that one in three people notice their phone is missing in under an hour
- There are already several options:
 - Mobile PKI (which we tried, <http://bit.ly/mobile-pki>)
 - SMS authentication
 - A host of 'Apps'
 - SIM add-ons like Vasco DigiPass Nano

One Friday afternoon...

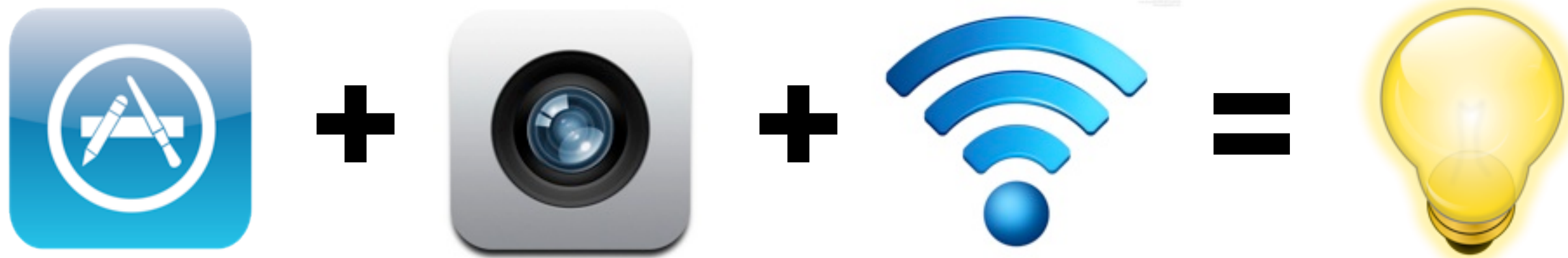
- As these things go, we started brainstorming...



- What we most dislike about almost all solutions:

Having to re-type complicated codes

- So one Friday afternoon in September we started thinking...





Seeing is believing ;-)

atiqr

DEMONSTRATION



Even cooler demo




How does it work?



Design and implementation

- Fully based on Open Standards
- Uses the OCRA suite developed by the Open Authentication (OATH) initiative
- Uses the HOTP algorithm (RFC 4226)
- AES 256-bit encryption
- Uses the ZXing QR-code library by Google
<http://code.google.com/p/zxing/>
- QR code patent is royalty free

Comparison of AuthN tech.

Method	Hardware Indep.	Software Indep.	Security	Cost	Open Standards	Ease-of-use
Username/ Password	++	++	--	++	=	+/-
OTP token	-	-	++	--	-/=	+
C/R token	-	-	++	--	-/=	+
PKI Token	--	--	++	--	=	+
Mobile PKI	+	+	++	?	+	++
SMS OTP	+	=	X	-	--	-
OTP Apps	+	+/=	+	+/=	+/=	=
	+	+/=	+	+	++	++

Security audit

- We contracted an external auditor
- Goals of the audit were:
 - White box security testing
 - tiqr architecture and design analysis
 - Code audit
- The audit was performed earlier this year
- We got good feedback and fixed some issues
- Status now: tiqr is a secure solution
- Read the report: <https://tiqr.org/audit/>





tiQR roadmap



- Available on Apple's App Store



- Available on Android Market



- Release as Open Source



- Security & code audit



- Partner with other solutions

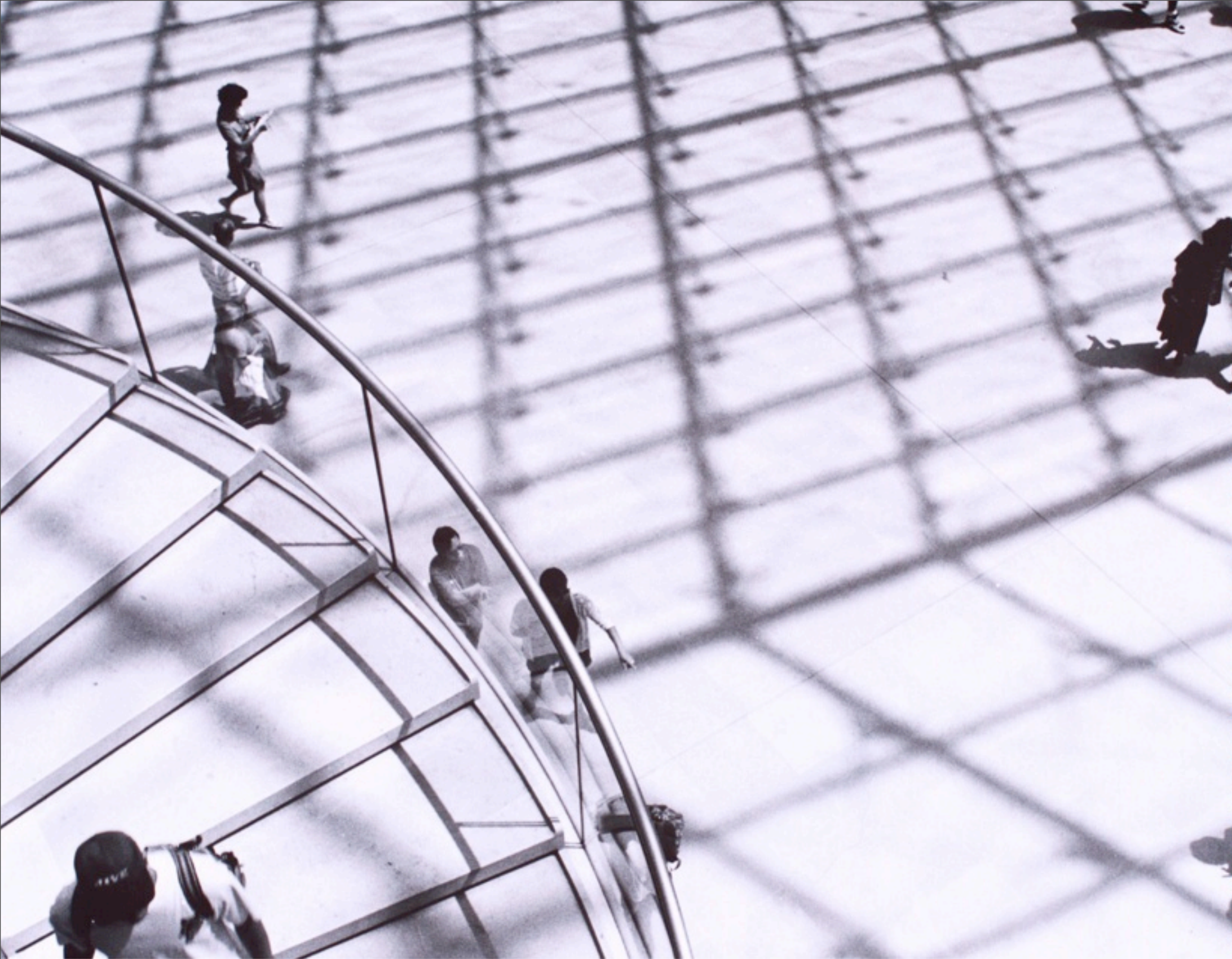
in progress

- Other mobile platforms

you? we?

- Pilot with "real users"

Q4 2011 -
Q1 2012



SURF
NET



**Questions? Comments?
Please contact me or visit
<https://tiqr.org/>**



roland.vanrijswijk@surfnet.nl



nl.linkedin.com/in/rolandvanrijswijk



@reseauxsansfil

