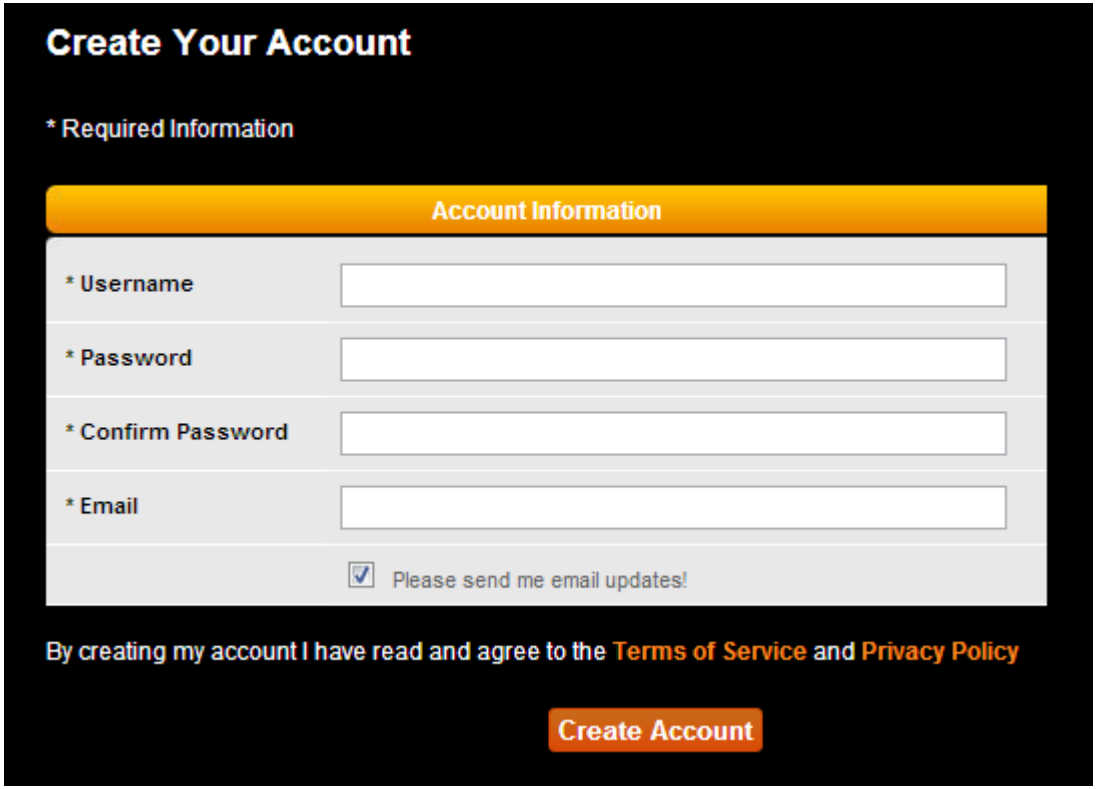
Beyond password:
Time for a change

Olivier Potonniée
Octobre 2013

How can web applications authenticate their online users?

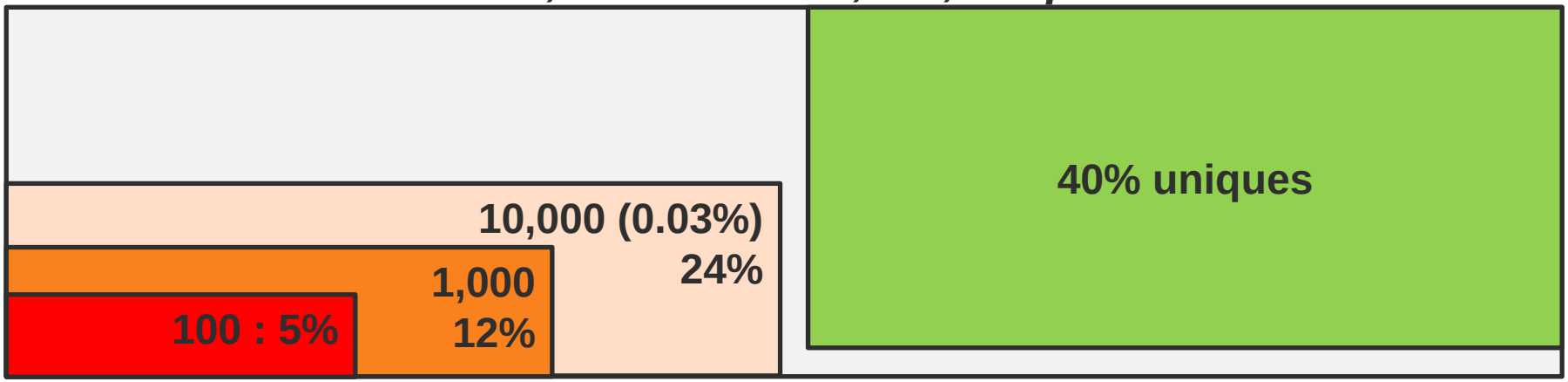
Often…



gemalto

Passwords?

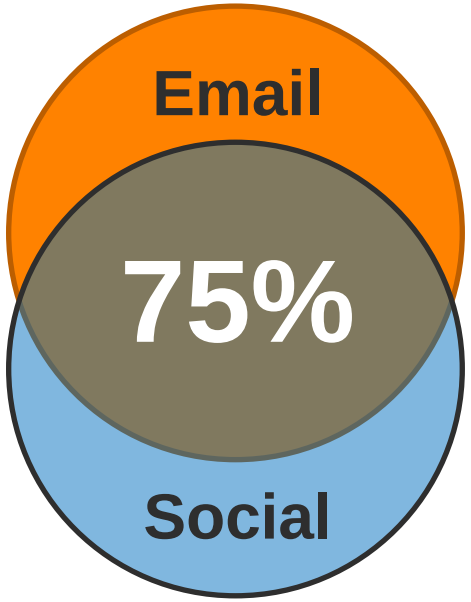
RockYou social network, Dec 2009: 30,000,000 passwords



gemalto

Attacks

- Compromised passwords in 2013:
  - Living Social: 50 millions
  - EverNote: 50 millions
  - Drupal: 1 million
  - Twitter: 250,000
  - …



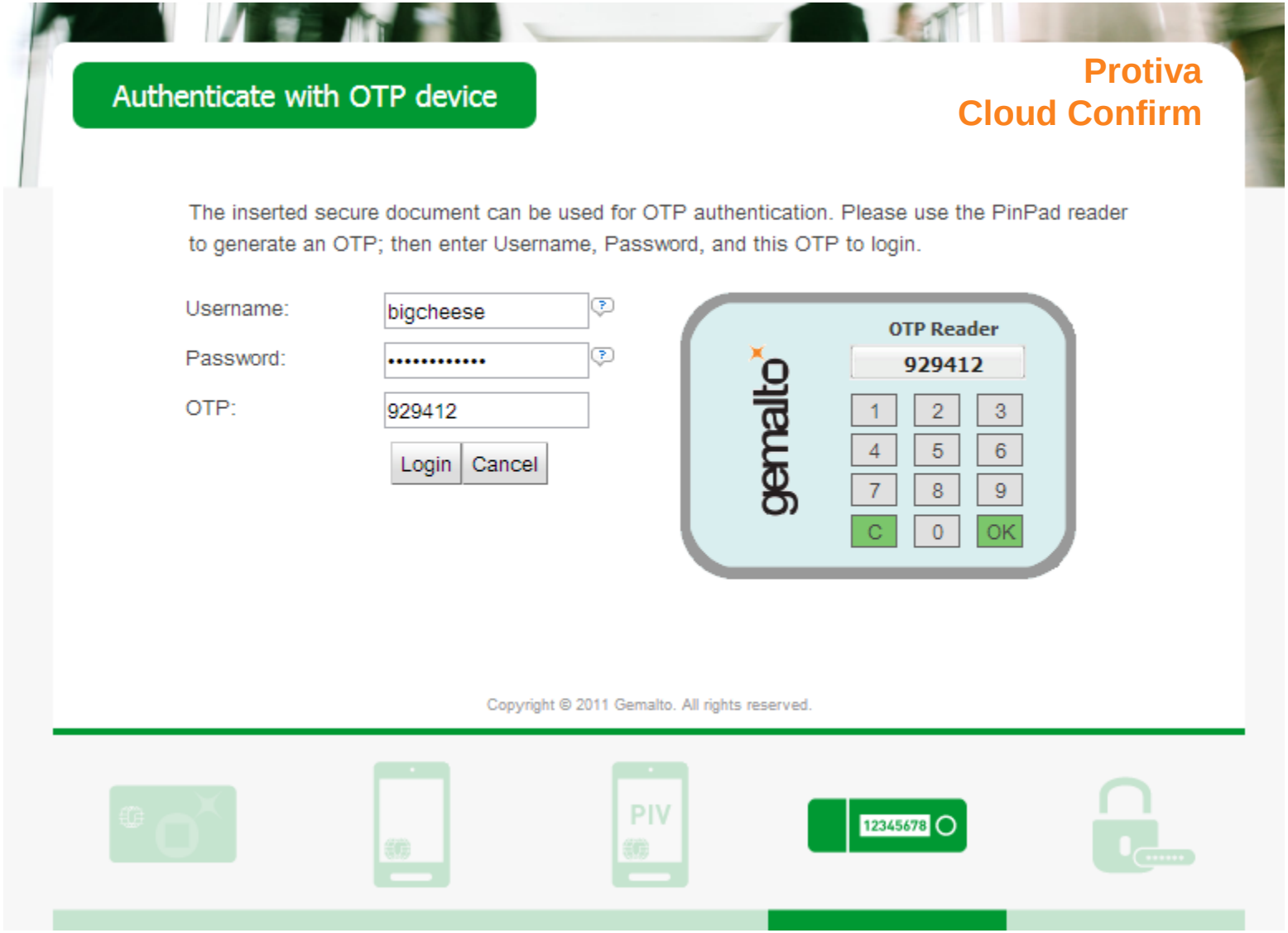
(BitDefender)

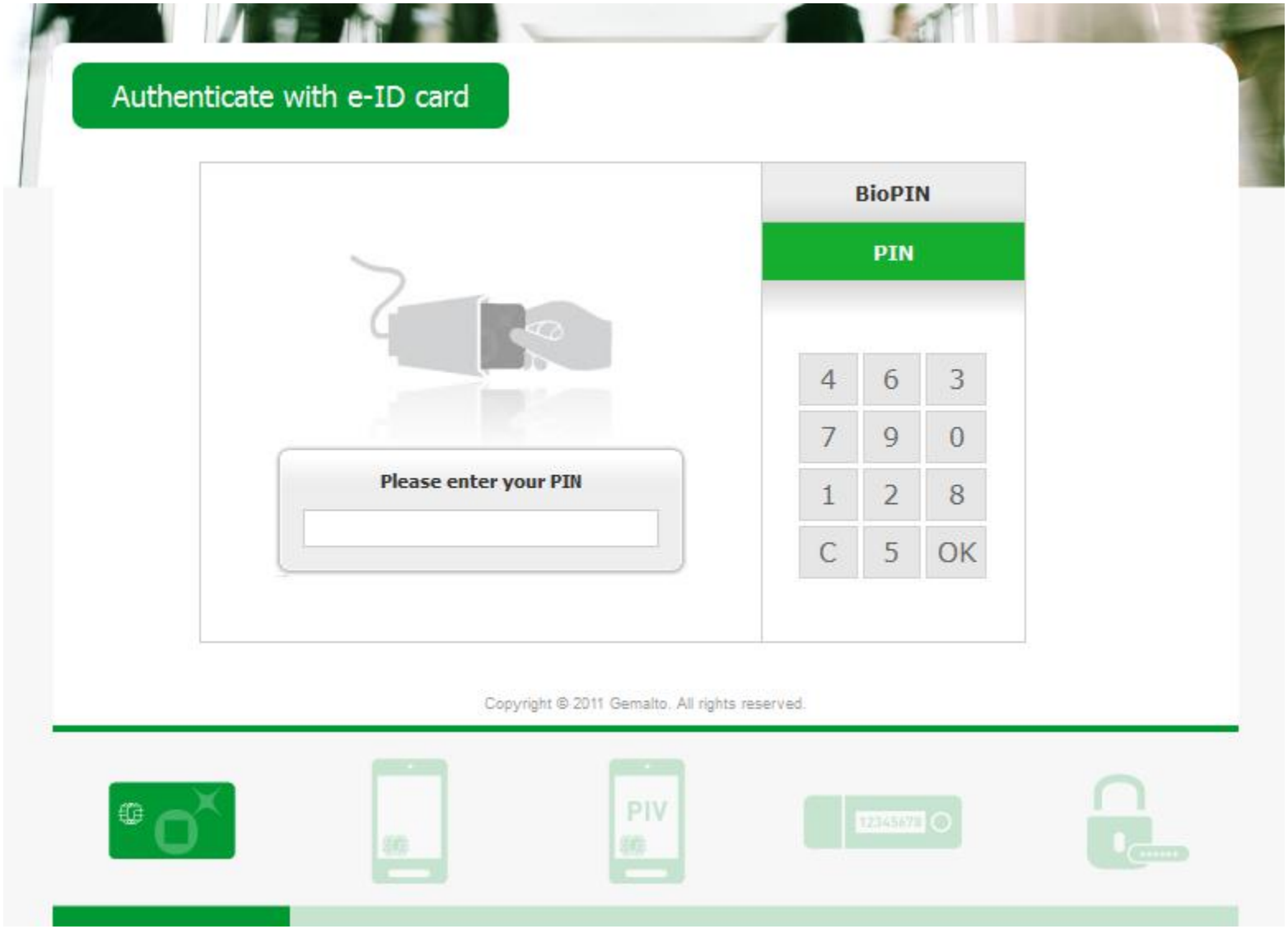
gemalto

Strong Authentication

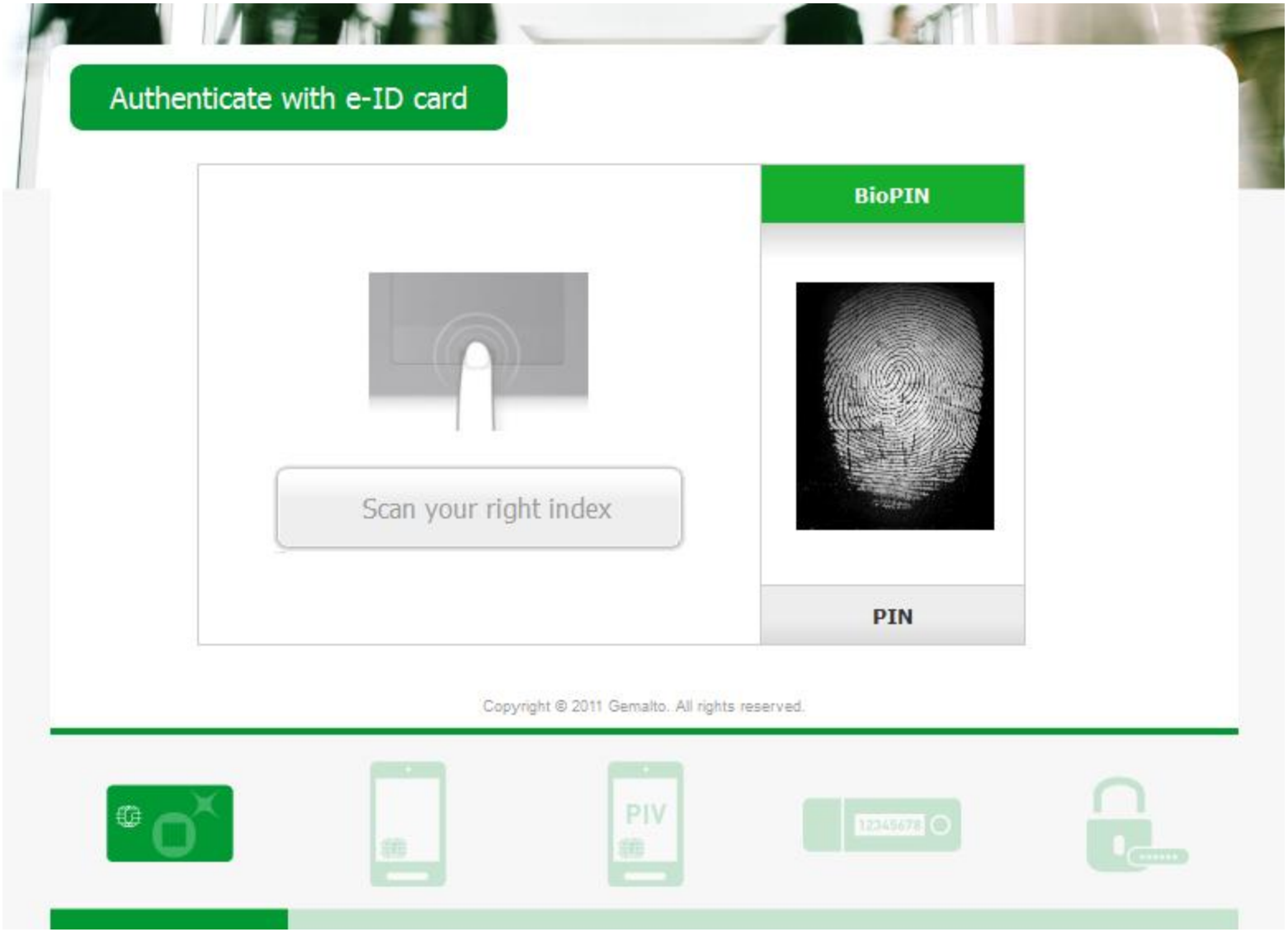
- At least 2 of:
  - Something you know (password, pin, etc.)
  - Something you have (card, mobile, etc.)
  - Something you are (biometrics)

- Independents, protected

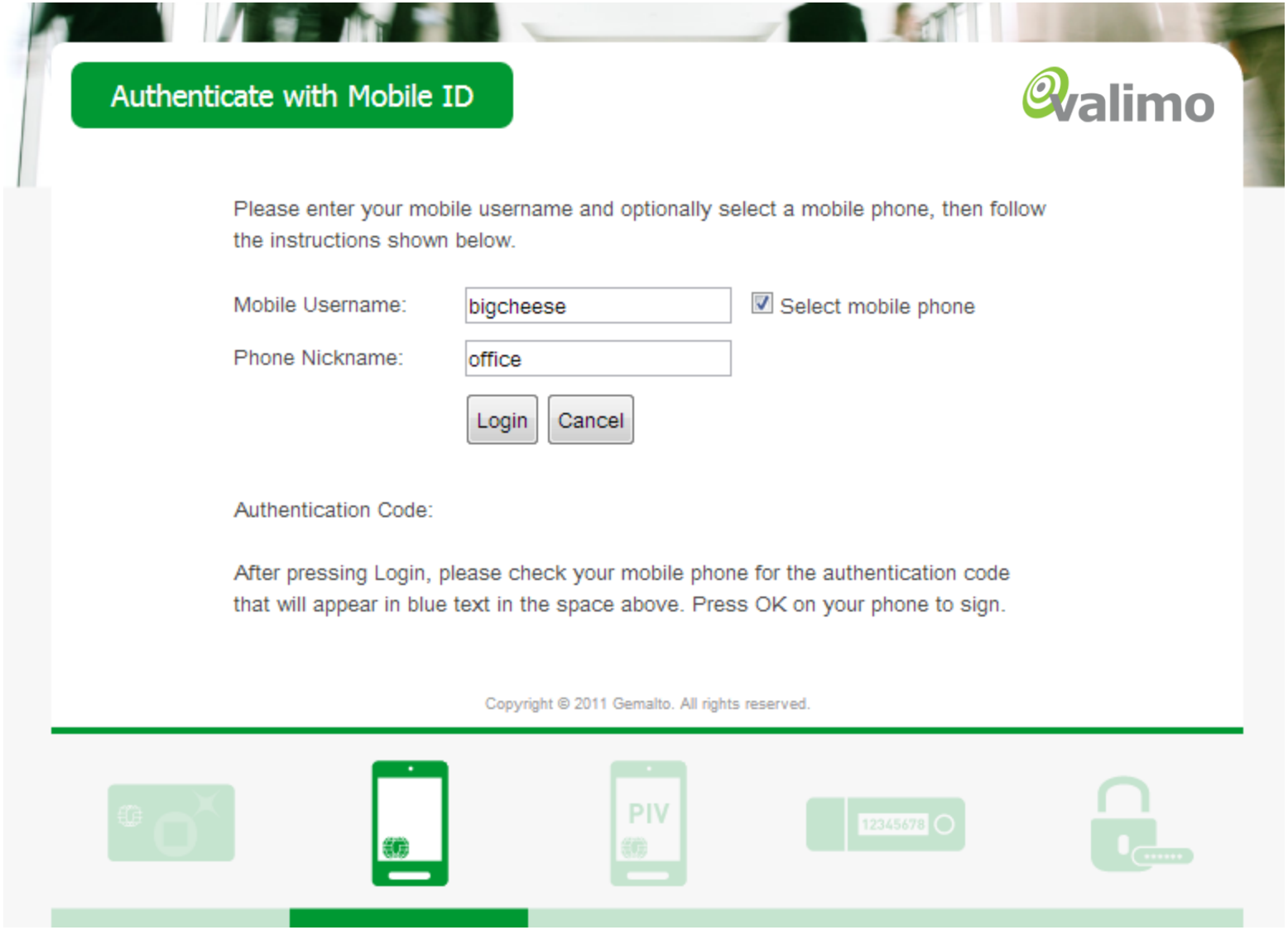

Authenticate with OTP device
Protiva
Cloud Confirm
The inserted secure document can be used for OTP authentication. Please use the PinPad reader to generate an OTP; then enter Username, Password, and this OTP to login.
Username:
bigcheese
Password:
OTP:
929412
Login
Cancel
OTP Reader
929412
1
2
3
4
5
6
7
8
9
C
0
OK
gemalto
Copyright © 2011 Gemalto. All rights reserved.
PIV
12345678


Authenticate with e-ID card
BioPIN
PIN
4 6 3
7 9 0
1 2 8
C 5 OK
Please enter your PIN
Copyright © 2011 Gemalto. All rights reserved.
PIV

gemalto

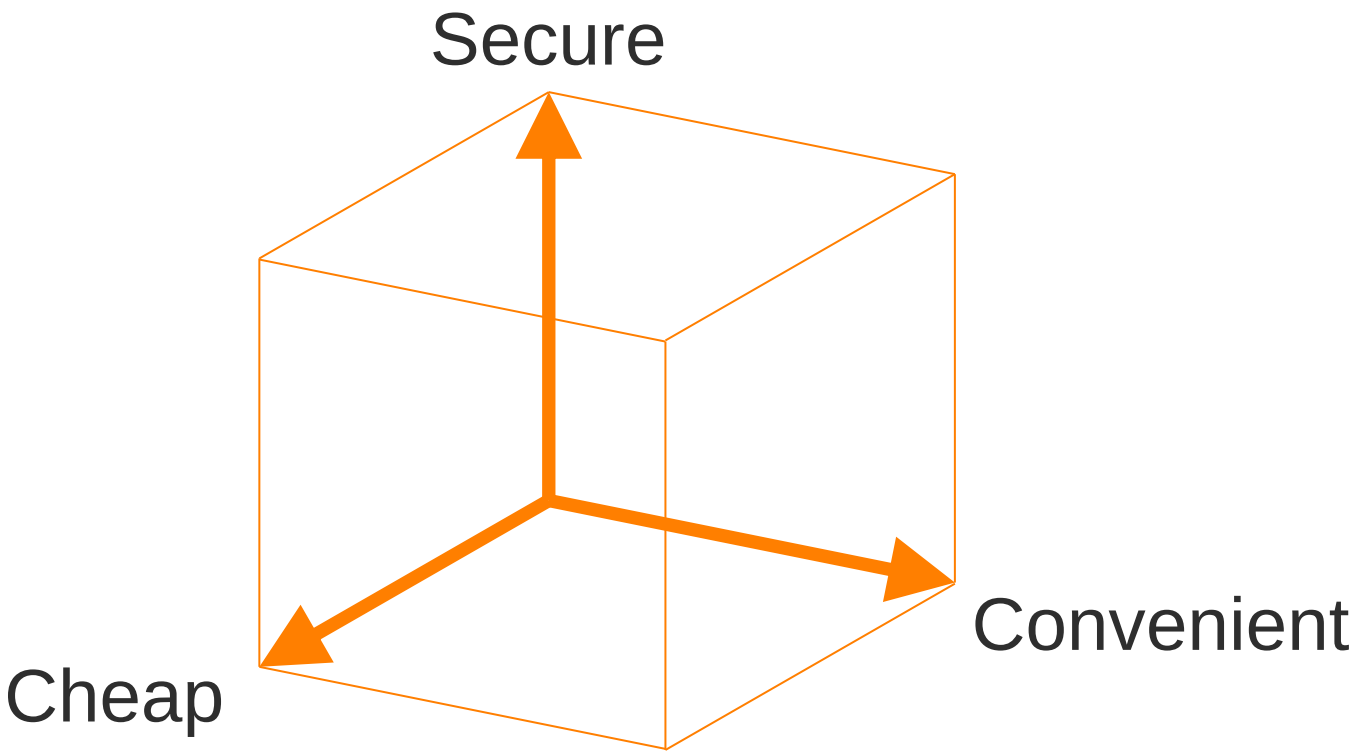

Authenticate with e-ID card
BioPIN
Scan your right index
PIN
Copyright © 2011 Gemalto. All rights reserved.
PIV

gemalto


Authenticate with Mobile ID
valimo
Please enter your mobile username and optionally select a mobile phone, then follow the instructions shown below.
Mobile Username:
bigcheese
Select mobile phone
Phone Nickname:
office
Login
Cancel
Authentication Code:
After pressing Login, please check your mobile phone for the authentication code that will appear in blue text in the space above. Press OK on your phone to sign.
Copyright © 2011 Gemalto. All rights reserved.
PIV
12345678

gemalto

Need to define YOUR solution



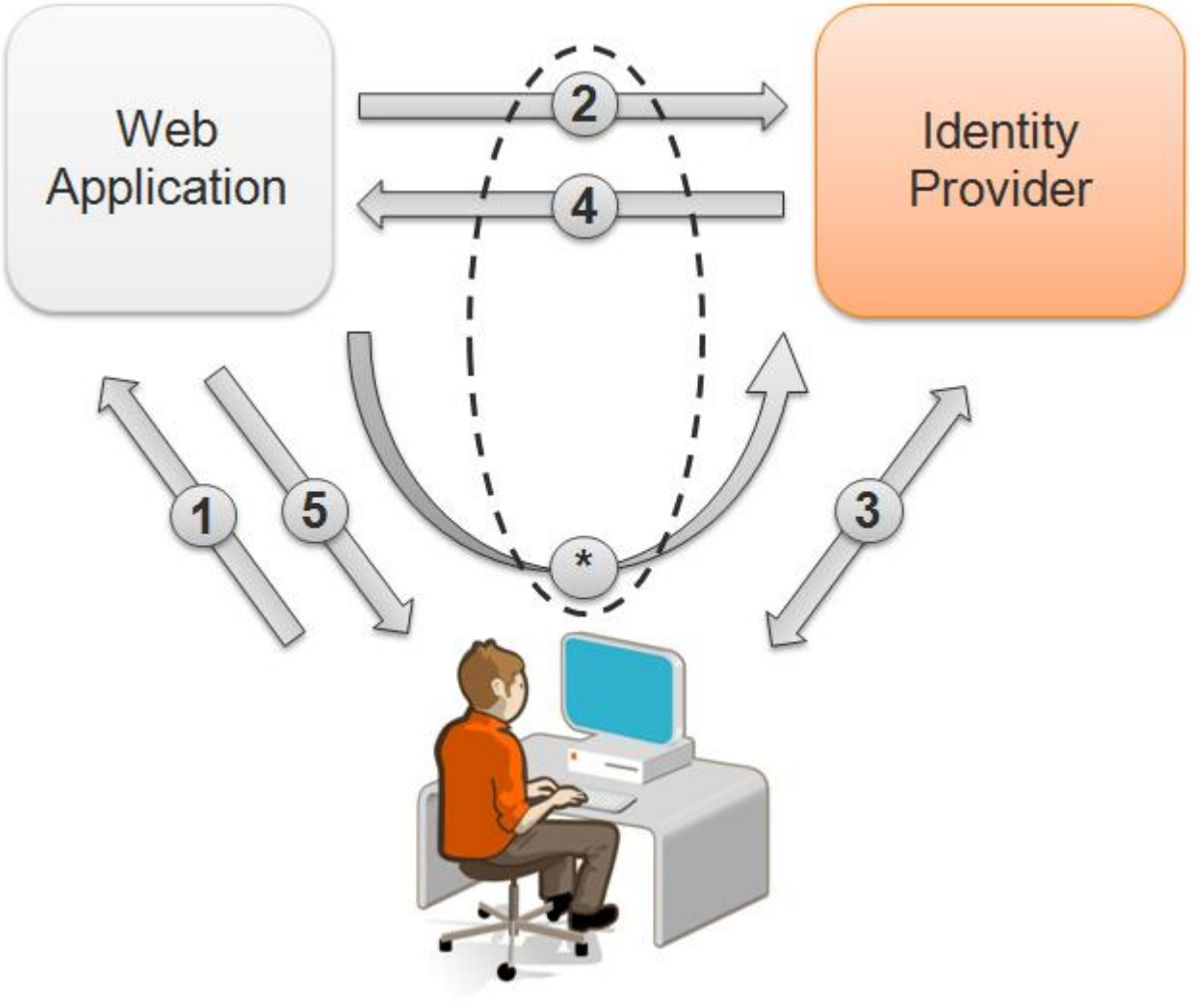
gemalto

Social Login

- Identity reuse
  - Simpler for users (no new identifier to remember)
  - Single-Sign-On (SSO)
- Alleviate the application
- Privacy risks
  - Traceability
  - Disclosure of personal data

gemalto

Authentication delegation



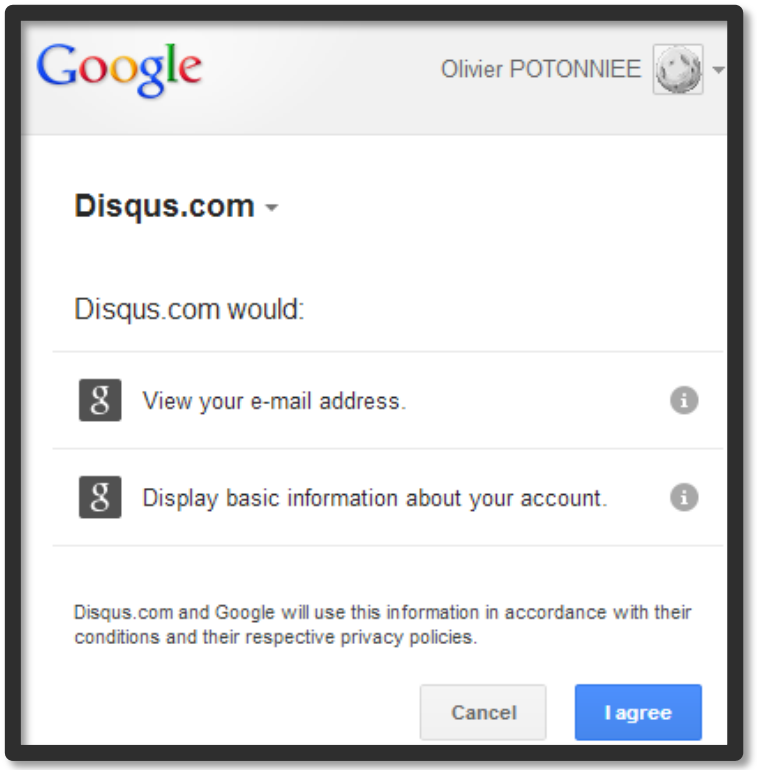
gemalto

Delegation protocols

OAuth

gemalto

OpenID A simple URL

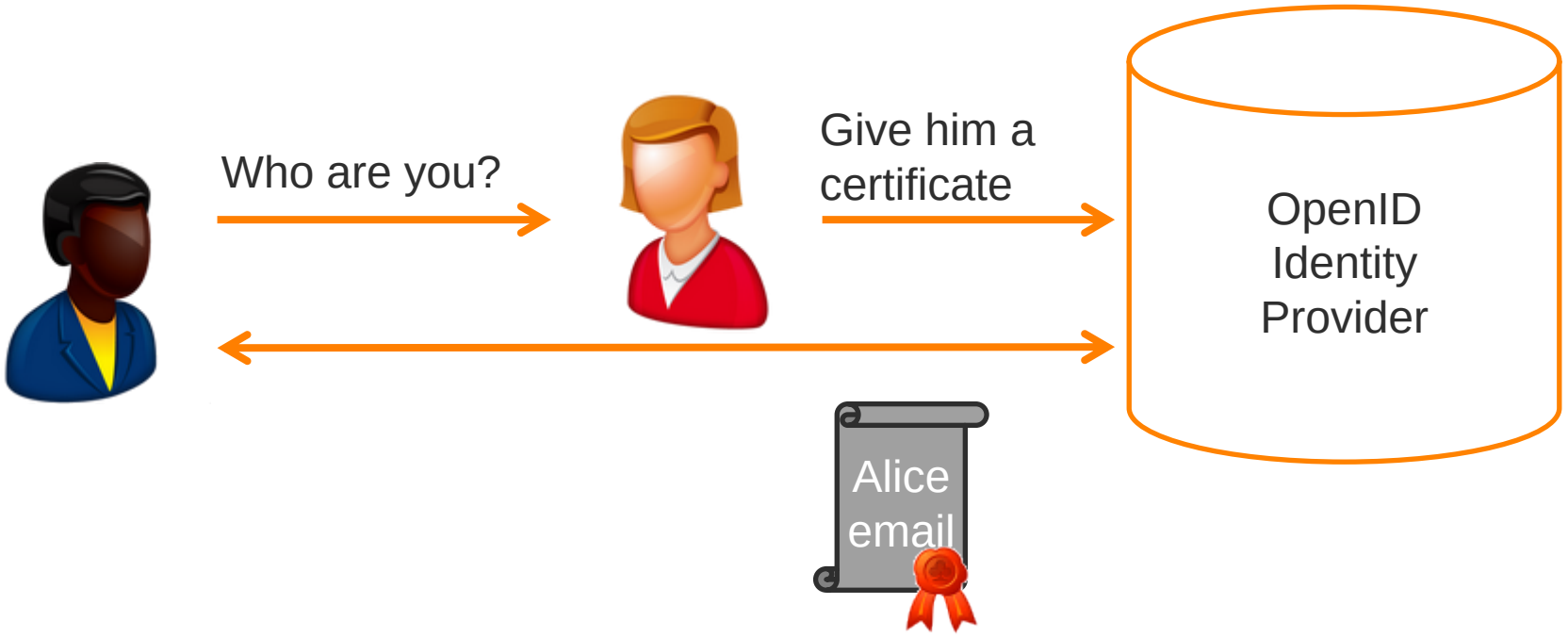


stackoverflow
Slashdot
sourceforge
Drupal

Google
YAHOO!
orange
WordPress
Aol.
claimID
VeriSign Labs

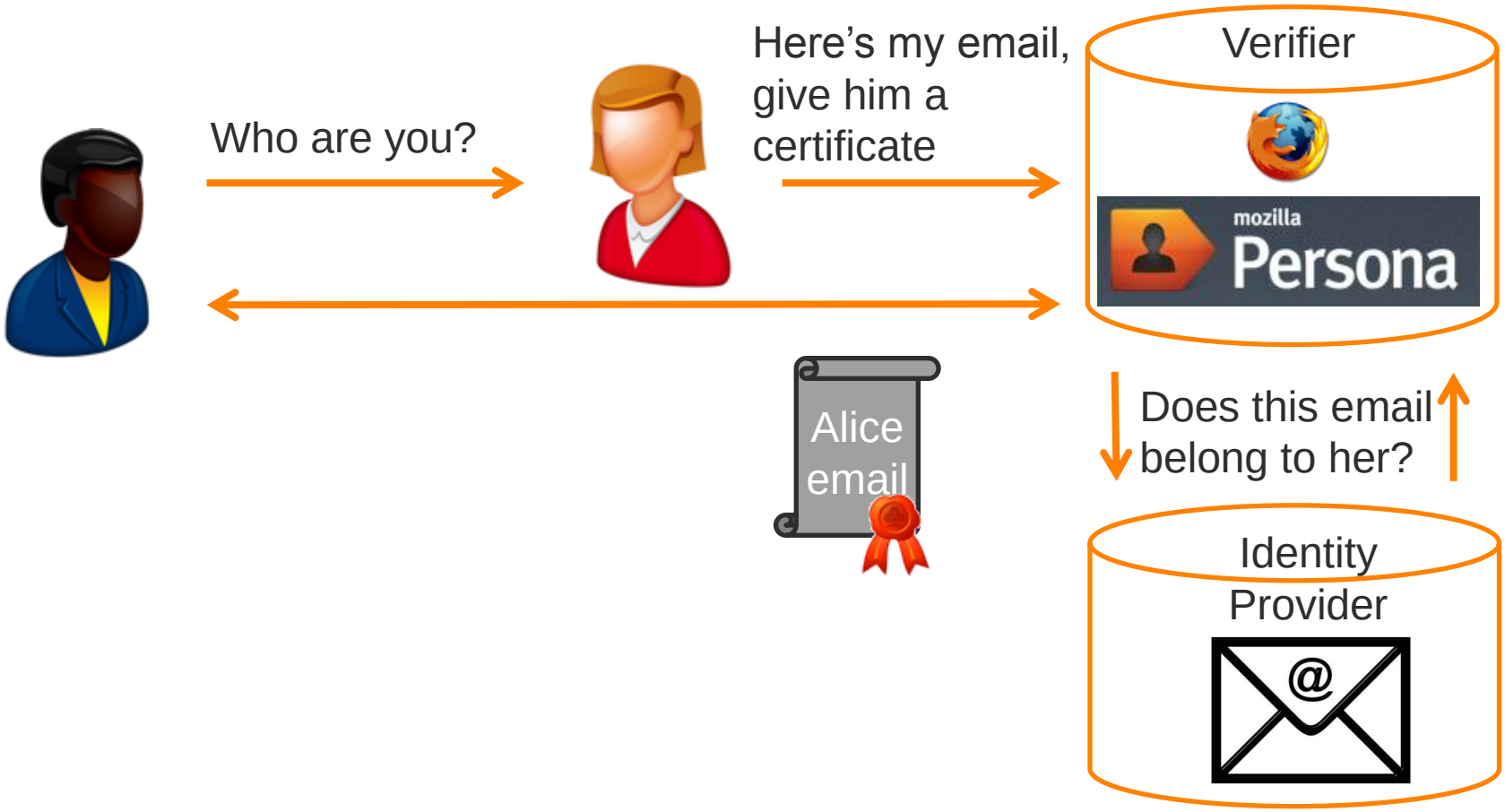
gemalto

Authentication

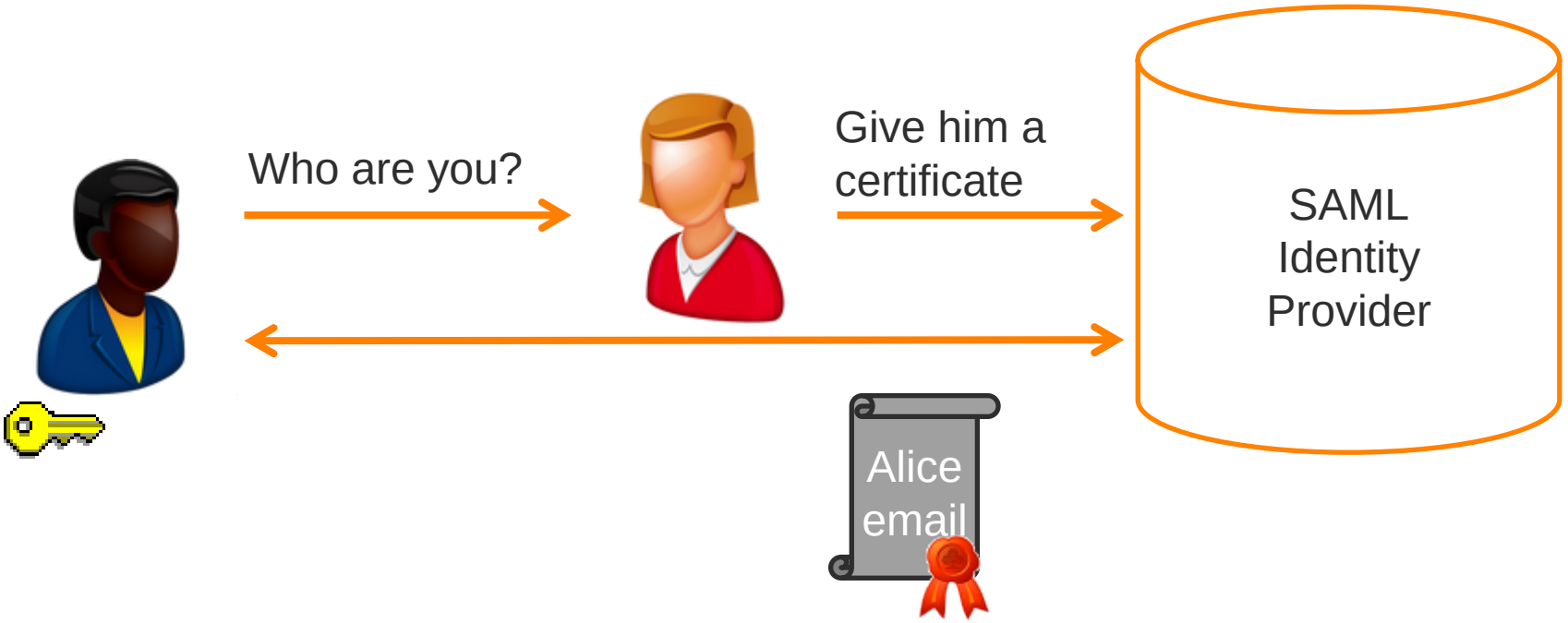


(nat sakimura)

Authentication via email

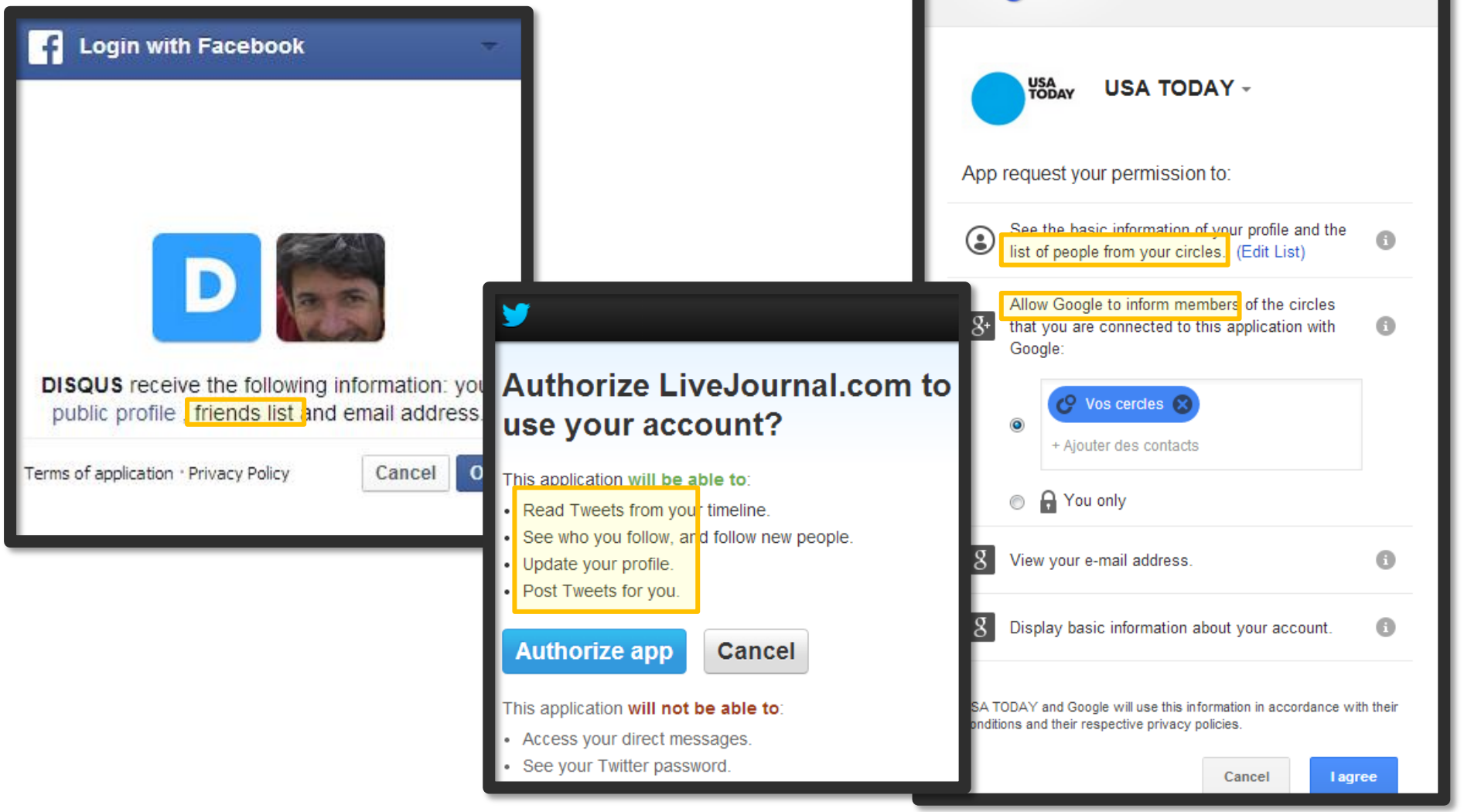


OASIS SAML Assertions



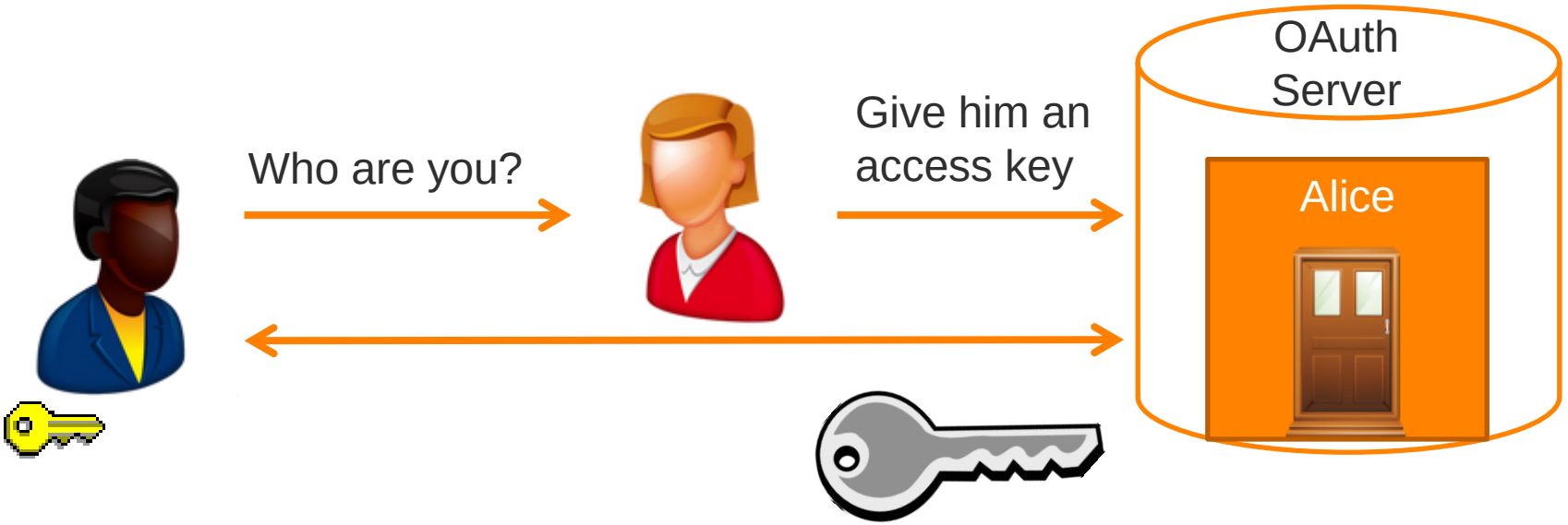
gemalto

OAuth Authorization to access personal data



gemalto

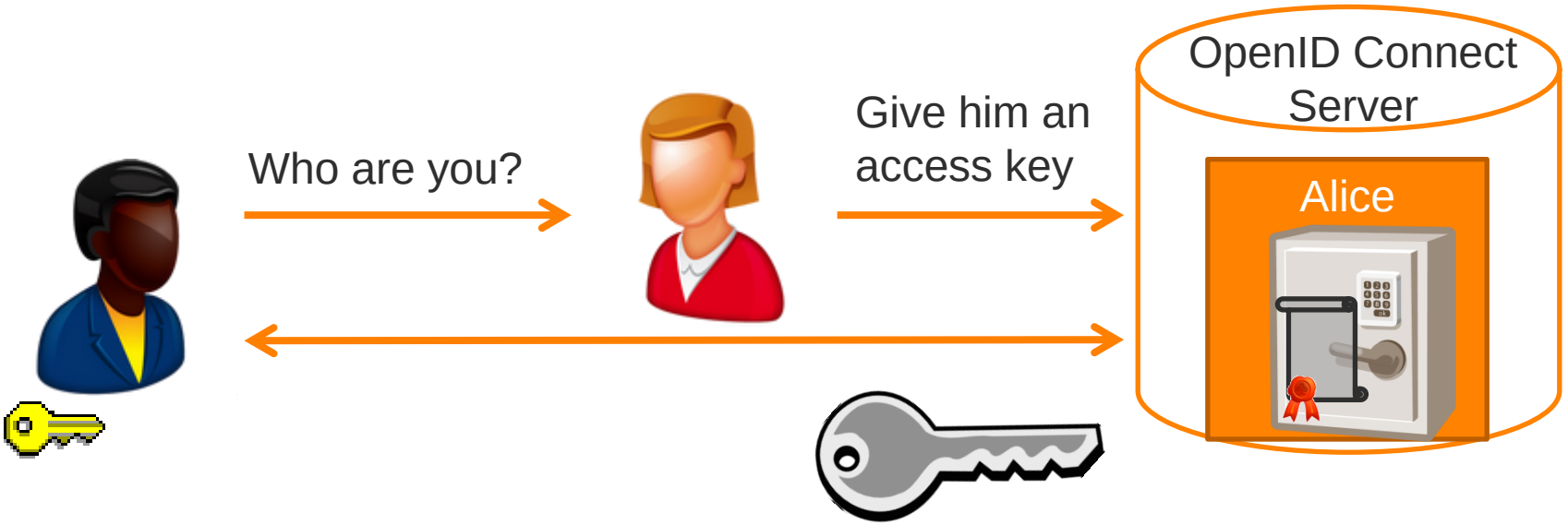
OAuth Authorization



gemalto

OpenID Connect

Authorization to access identity



gemalto

Define YOUR solution

- Confidentiality / Personal data sharing?
- Pre-registration of web application?
- Dependency to an identity provider?
- Authentication methods?

THE Message

- Passwords are bad
  - Strong Authentication
- Too many identities is inconvenient
  - Reuse identities (emails, social networks…)
- Authentication is a sensitive and potentially complex task
  - Delegation, SSO
- Privacy needs to be protected
  - Don’t ask for more data or access rights than needed

Thanks