



IDENTITY, PRIVACY AND SECURITY

Jaya Baloo

Professional Services - IAM Secure Mobility & Consumer IDM

Verizon Business

May 25, 2012



Consumer & Commercial Identity Management Challenge

People



	Service	Username	Authentication Mechanism
1	Gmail/IMFT Mail	Email address	Password
2	Bank Account	Account number	Password (Shared Secret)
3	401K	Account number	Password (Shared Secret)
4	Brokerage	Account number	Password (Shared Secret)
5	Cell phone	Email address	Password (Shared Secret)
6	Home Insurance	Account number	Password (Shared Secret)
7	Home Cable and Phone	Email address	Password (Shared Secret)
8	Hotwire	Email address	Password (Shared Secret)
9	Travelocity	Email address	Password (Shared Secret)
10	LinkedIn	Email address	Password (Shared Secret)
11	Facebook	Email address	Password (Shared Secret)
12	Twitter	Email address	Password (Shared Secret)
13	Marriott Rewards	Account number	Password (Shared Secret)
14	United Airlines	Account number	Password (Shared Secret)
15	Apple or online Music	Email address	Password (Shared Secret)
16	Industry Certification	Email address	Password
17	Kuerig Coffee	Email address	Password (Shared Secret)
18	Best Buy	Email address	Password (Shared Secret)
19	eBay	Email address	Password (Shared Secret)
20	Paypal	Email address	Password (Shared Secret)
21	Comidental	Account number	Password (Shared Secret)
22	AIM/IM	Email address	Password (Shared Secret)
23	ezpass	Account number	Password (Shared Secret)
24	Work Portal	User ID	Password (Token)
25	Work email	User ID	Password (Token)
26	Work Partner Portal	User ID	Password (Token)
27	Industry Association	User ID	Password

- Too many passwords
- Too much complexity
- Too much risk
- Simply too hard
- Identity fraud

Enterprises









- Highly complex
- Too expensive
- Too much risk
- Not enough flexibility
- No scalability

Isn't it time the internet had an identity solution?

Identity Spotlight

The Market Needs a Better Solution

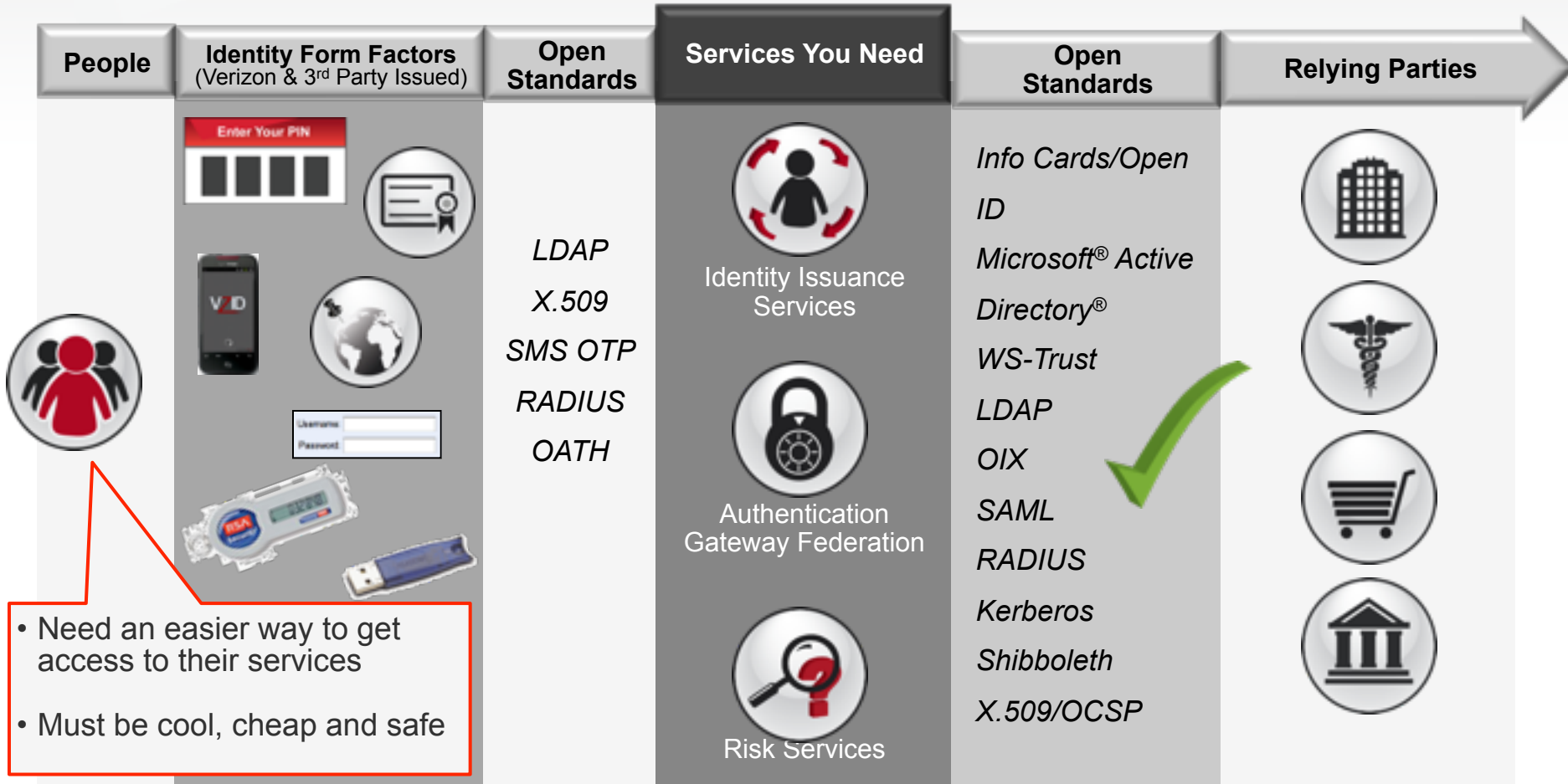
•ACCORDING TO GARTNER, ONE OF THE FOLLOWING MUST OCCUR:

- 1 •Identity providers find a beneficial business model
•For issuing general-use credentials. 
- 2 •Governments, enterprises pay identity providers
•To perform identity proofing to issue credentials
•To and authenticate constituents.   
- 3 •A network of organizations emerges that can
•produce appropriate identity assurance by:
-- Providing individual identity attributes/claims proofing services
-- Creating a reliable "built-up" network identity-proofing score²  

•“Real success for these frameworks will come when they can be used for a wide variety of contexts with different risk profiles—social, consumer, enterprise and business-to-business.”

² Kreizman, Gregg, Ray Wagner and Earl Perkins. "Open Identity Pilot Advances the Maturity of User-Centric Identity, but Business Models Are Still Needed." Gartner, November 9, 2009. <http://www.gartner.com/DisplayDocument?d=1223830>. ID Number: G00172278

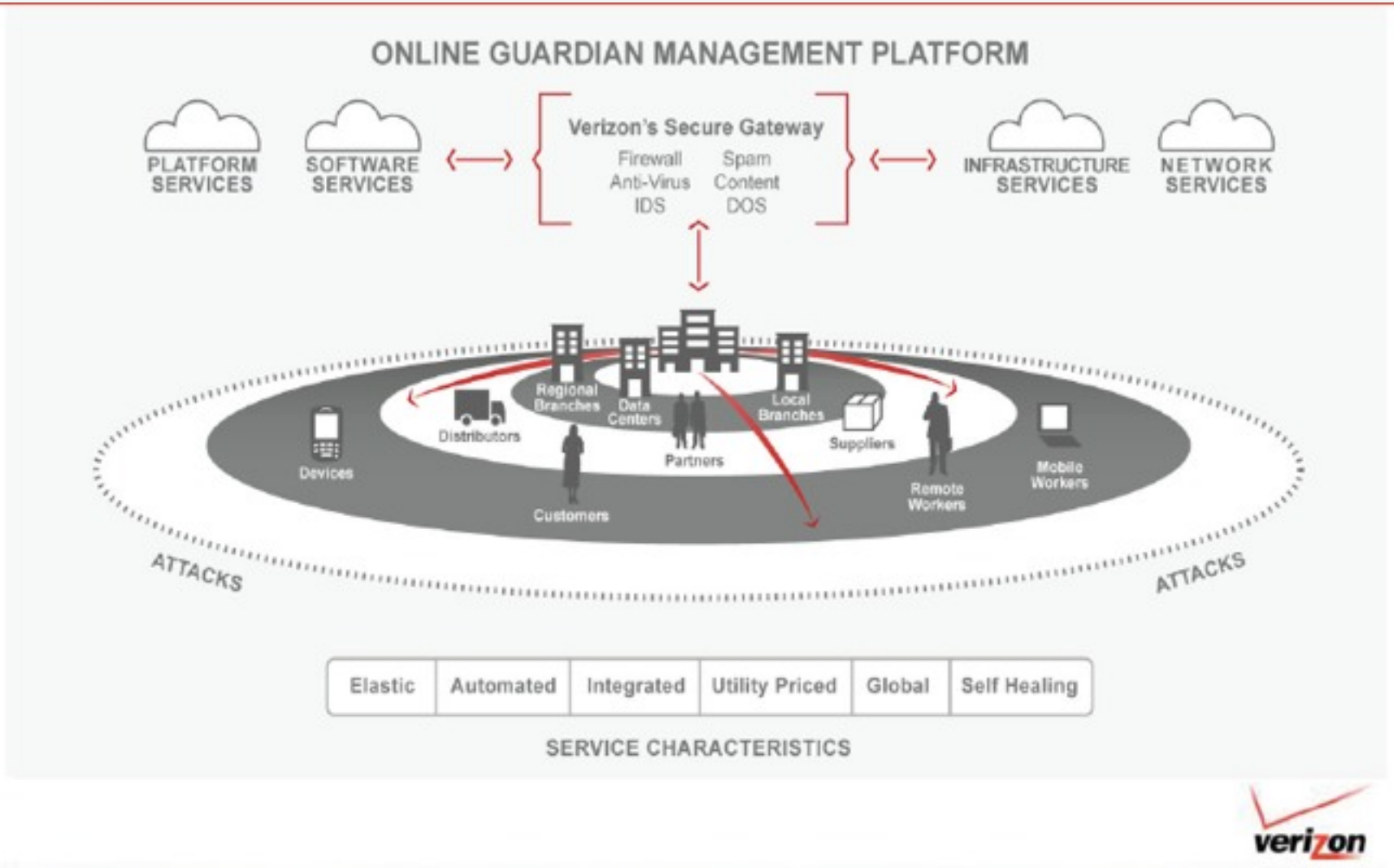
The Cloud Identity Problem



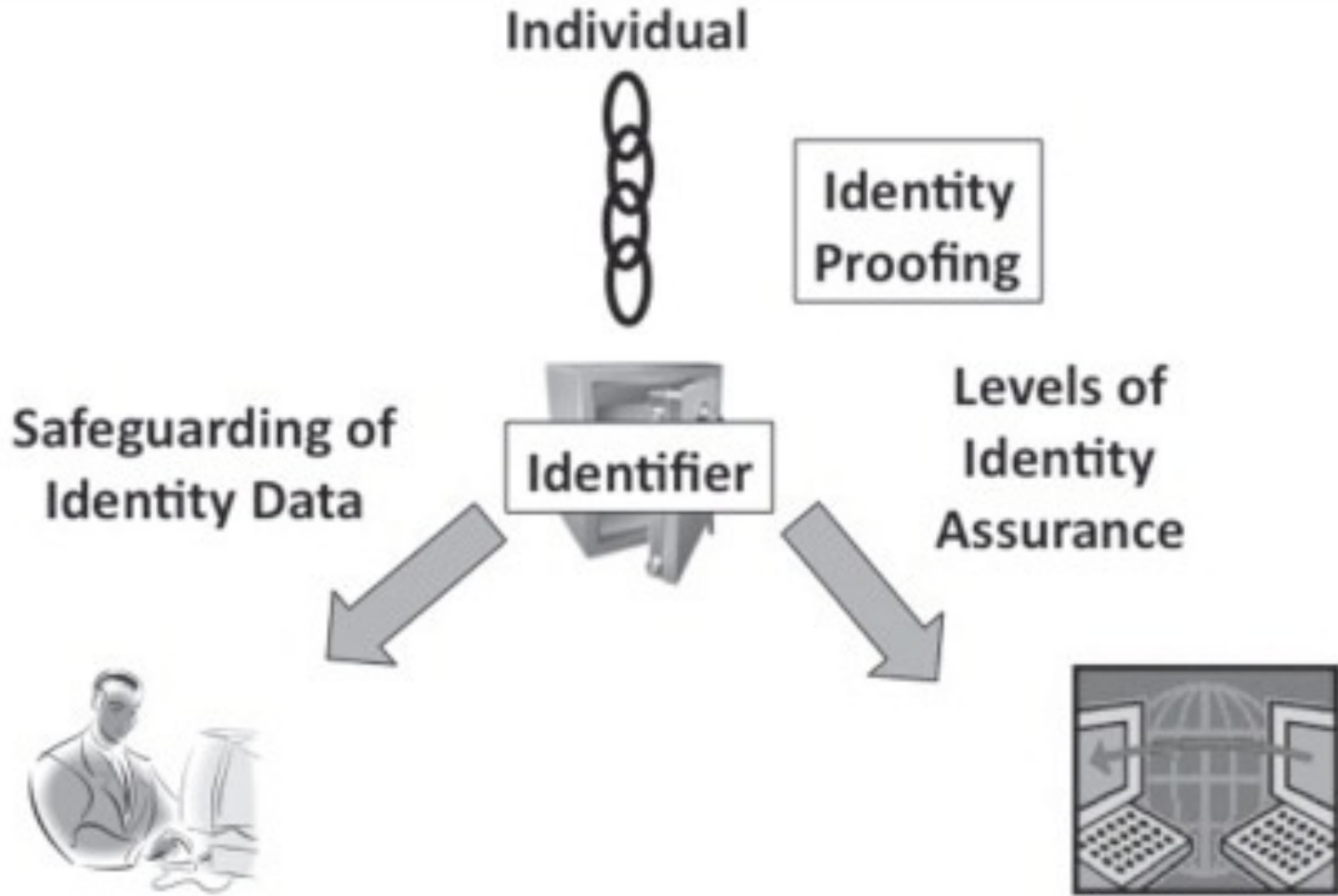
We need an identity ecosystem in the cloud.



Addressing Cloud Services and Security Challenges light of MOCLO era



Summary of the Challenge



Privacy Assurance

Identity Assurance

Sign In [or Register](#)

Welcome, share what's interesting to you.

Email

Password

Remember me

Sign In

[Forgot password?](#)

[Need help?](#)

Or, use...

Facebook

- Facebook
- Twitter
- Google
- MySpace
- Yahoo!
- AOL/AIM
- Blogger
- LiveJournal
- WordPress.com
- OpenID

Claims based authentication example

Block or unblock 18+ content on mobiles

We respect our customer's freedom to choose what material they access, but equally we want to protect our younger customers. Before you are able to view 18+ commercial content, you will have to prove that you are old enough.



The first time you use a credit card to prove to us that you are 18 or older we will charge £1 to your credit card and credit £1 to your mobile account. Please note that each time you age verify, your credit card will be charged £1. You will only receive £1 credit when you use this service for the first time.

To block or unblock access to 18+ content

Before you can block or unblock access to 18+ content, you need to enter your O2 mobile number and click continue. We will then instantly text you a verification code which you will need to enter on the next page to continue with the service settings.

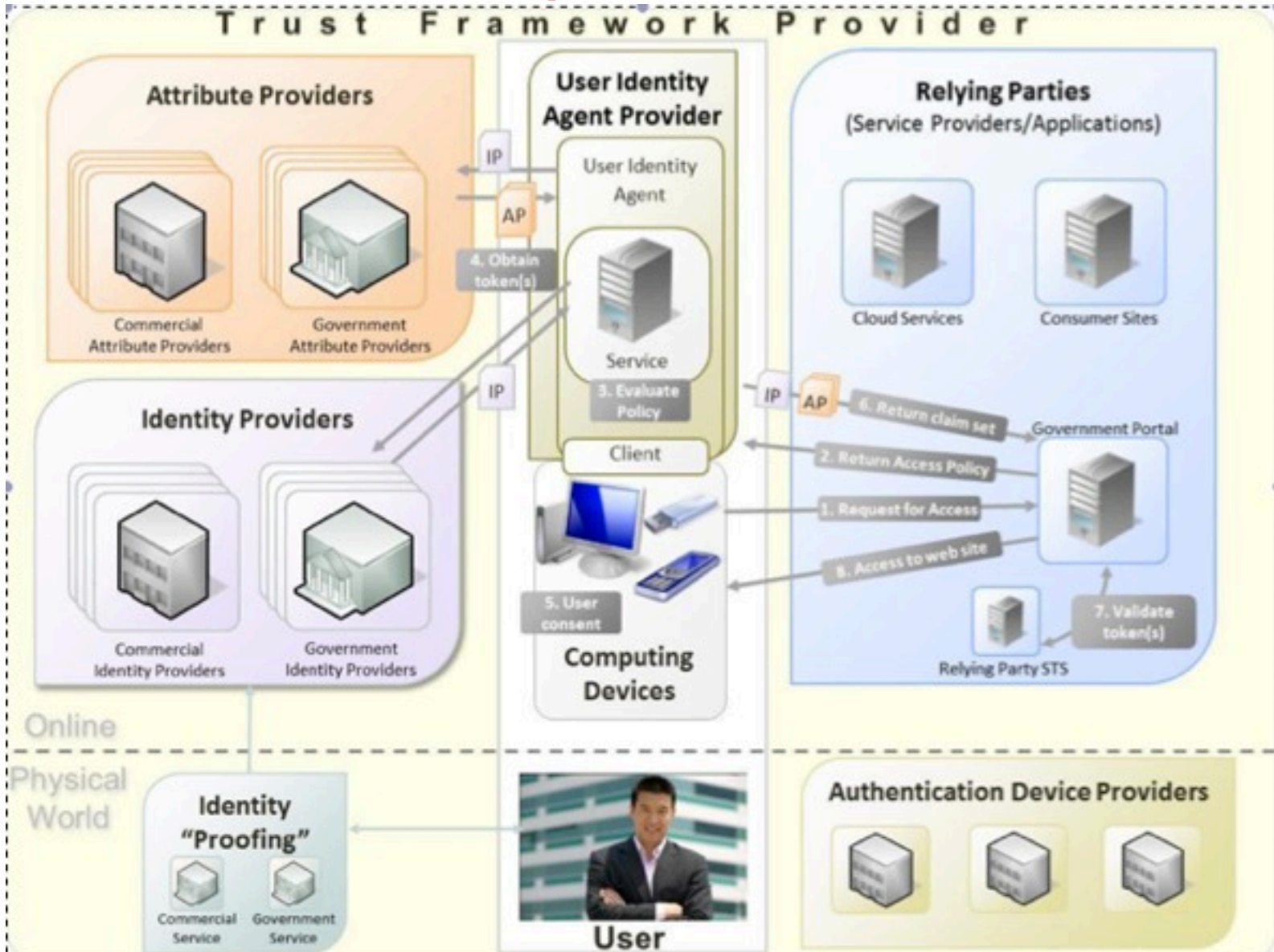
Enter your O2 mobile number: → Continue

Have you already received a text with your verification code?

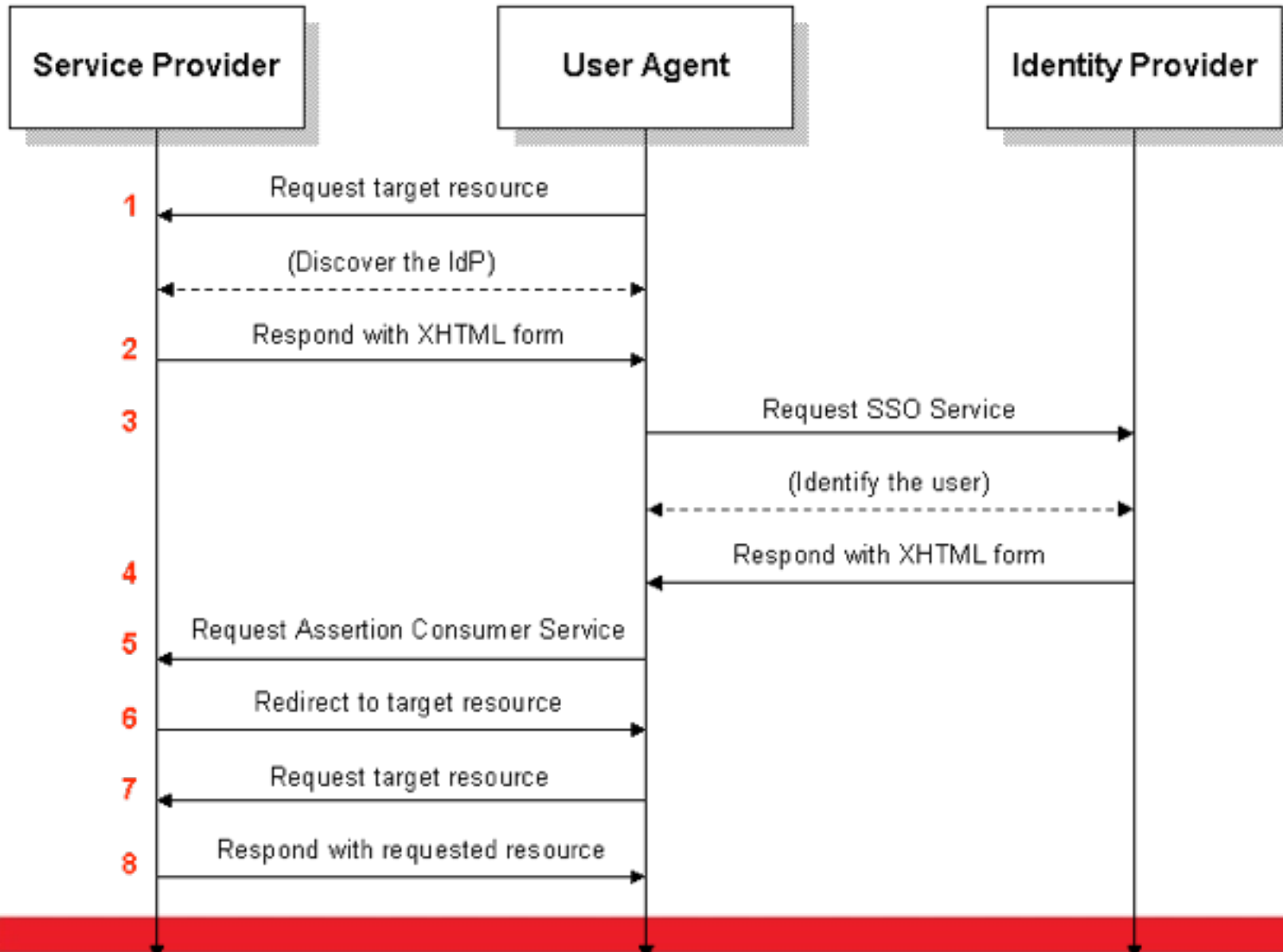
If you have already received your verification code click here to continue.

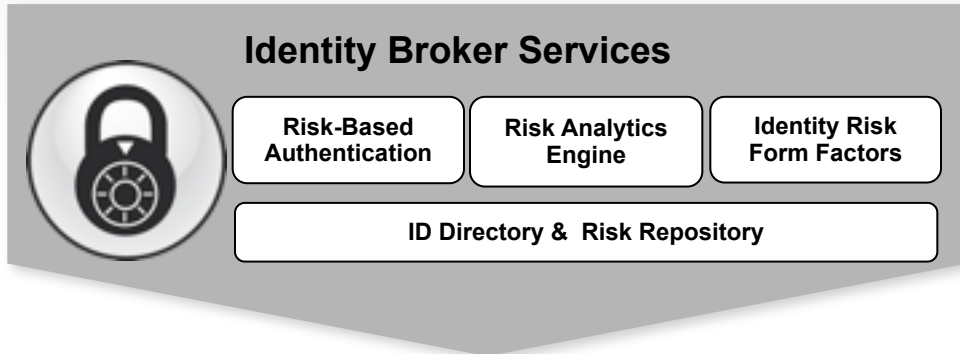
→ Continue

How does it work? Sample Architecture



How does it work? using SAML2 example





Tangible ID Form Factors

This section illustrates tangible ID form factors with various icons: a physical security token, a physical ID card, a smartphone displaying 'VZID', a USB drive, a document icon, a fingerprint icon, a login form with 'Username:' and 'Password:' fields, and a PIN entry screen with the text 'Enter Your PIN' and four input boxes.

Intangible ID Form Factors

This section illustrates intangible ID form factors with icons: a globe with a key, a profile of a person with sound waves (representing voice), a keyboard with a hand typing (labeled 'Key-stroke Biometrics'), and an IP address '192-168-1-2' with a red prohibition sign over it.

- “Every digital subject has a limited number of identity attributes.
- Attributes are acquired and contain information about a subject, such as medical history, purchasing behavior, bank balance, age and so on.
- Preferences retain a subject's choices such as favorite brand of shoes, preferred currency.
- Traits are features of the subject that are inherent, such as eye color, nationality, place of birth. While attributes of a subject can change easily, traits change slowly, if at all.”



What If We Had an ID Risk Score?

Primary Authentication Factor

Verification of user's Primary Authentication credential – provides base ID Risk Score

Sample Risk Score Components

- ID Proofing Assurance Levels (1 – 4)
- Credential Type Levels (1 – 4)



Location & Behavioral Factors

Addition of IP Malice and other historical behavioral factors – increases or reduces ID Risk Score based on factors identified

Sample Risk Score Components

- IP Malice
- IP Location History
- User IP Velocity History



Supplemental Authentication Factors

Addition of supplemental Authentication Factors focused on verifying that the intended user is in control of the Primary Authentication Factor – used when necessary to increase ID Risk Score to meet an application threshold

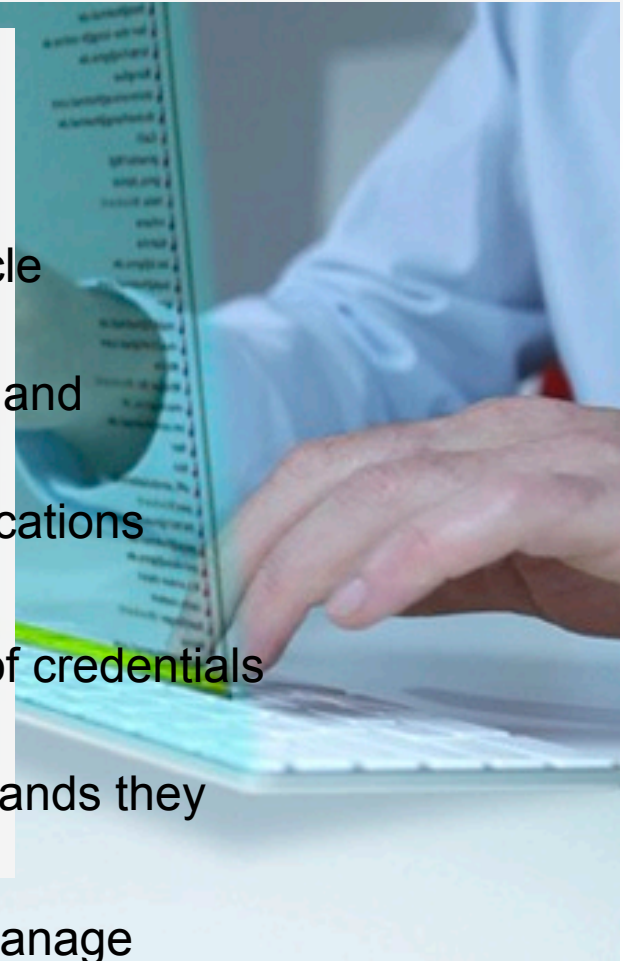
Sample Risk Score Components

- Mobile phone geo-location
- SMS OTP
- Static KBA
- DynaUIA KBA



Benefits from Controlling Costs, Complexity, and Risks

- Manage identity service operating costs
- Help reduce risks for identity fraud for individuals and for organizations
- Fast, efficient identity proofing and credential lifecycle management – credential users in minutes
- Positive user experience for credential provisioning and transactional authentication
- Standard authentication experience across all applications and services
- Ability for users to significantly reduce the number of credentials they manage – perhaps to a single credential
- Allows users to control how they interact with the brands they trust and only share the data that they specify
- Ability to get highly targeted offers and be able to manage loyalty management programs easily



- **(un)Traceability:** The degree to which a provider of digital identity information (a “claims provider”) can know where this information is used (at a “relying party”).
- **(un)Linkability from relying party to claims provider:** The degree to which a relying party can share transaction information with a claims provider to deterministically “link” transactions to a particular user.
- **(un)Linkability between relying parties:** The degree to which relying parties that share transaction information can deterministically “link” transactions at their respective sites to a particular user.
- **(non)Disclosure:** the degree to which specific pieces of digital identity information is disclosed for a given transaction. For example no disclosure whatsoever of age-related information, versus sharing a claim of “over 21,” versus sharing a full birth date.
- Legislation -White House release Bill of Privacy Rights“ (23.02.2012)Proposal for a new EU Data Protection Regulation Framework (25.1.2012)

Eagle Eye



Attributes as a commodity

<http://www.rapleaf.com/features/>



RapLeaf Personalization Data Segments Pricing and Availability

Segment	Field	Price ¹
<i>Rapleaf Core</i>		
1. Basic	Age	Free
2. Basic	Gender	Free
3. Basic	Location	Free
4. Premium	Household Income	\$0.01
5. Premium	Marital Status	\$0.01
6. Premium	Presence of Children	\$0.01
7. Premium	Home Owner Status	\$0.01
8. Premium	Home Property Type	\$0.01
9. Premium	Length of Residence	\$0.01
10. Premium	Home Market Value	\$0.01
11. PREMIUM BUNDLE	Income, Marital Status, Presence of Children, Home Owner Status, Home Property Type, Length of Residence, Home Market Value	\$0.05
12. Auto	Cars in Household	\$0.01
13. Auto	Vehicle New or Used	\$0.01
14. Auto	Vehicle Type	\$0.01
15. Financial	Likely to Use Financial Services	\$0.01
16. Financial	Invested Assets	\$0.01
17. Financial	Loan-to-Value Ratio	\$0.01
18. Financial	High Net Worth	\$0.01
19. Financial	Credit Card - Has Premium Credit Card	\$0.01
20. Financial	Credit Card - Has Retail Card	\$0.01



Why collect Identities and rich Attributes

- Two sided advertising-markets: personal data is the ,glue` to leverage high-priced ad-revenues that pay for most of the free content and services online
- Basis for shareholder value
- Facebook - Current stock market valuation: investors value each profile at approximately 90-120 USD*
- MySpace - Drama: Valuation dropped from \$ 12 billion (2007) to \$ 35 million (2011) as the crowd moved to Facebook *
- Privacy legislation is principally aimed at protecting the individual's personal information from misuse by governments and organizations. It does not help to protect the individual against their own mis-judgements or the organization against the mistakes of their employees.
- What if we had property rights for personal data or a mechanism to "sell attributes" about ourselves? (Trust in Digital Life)

A few Government Identity Initiatives



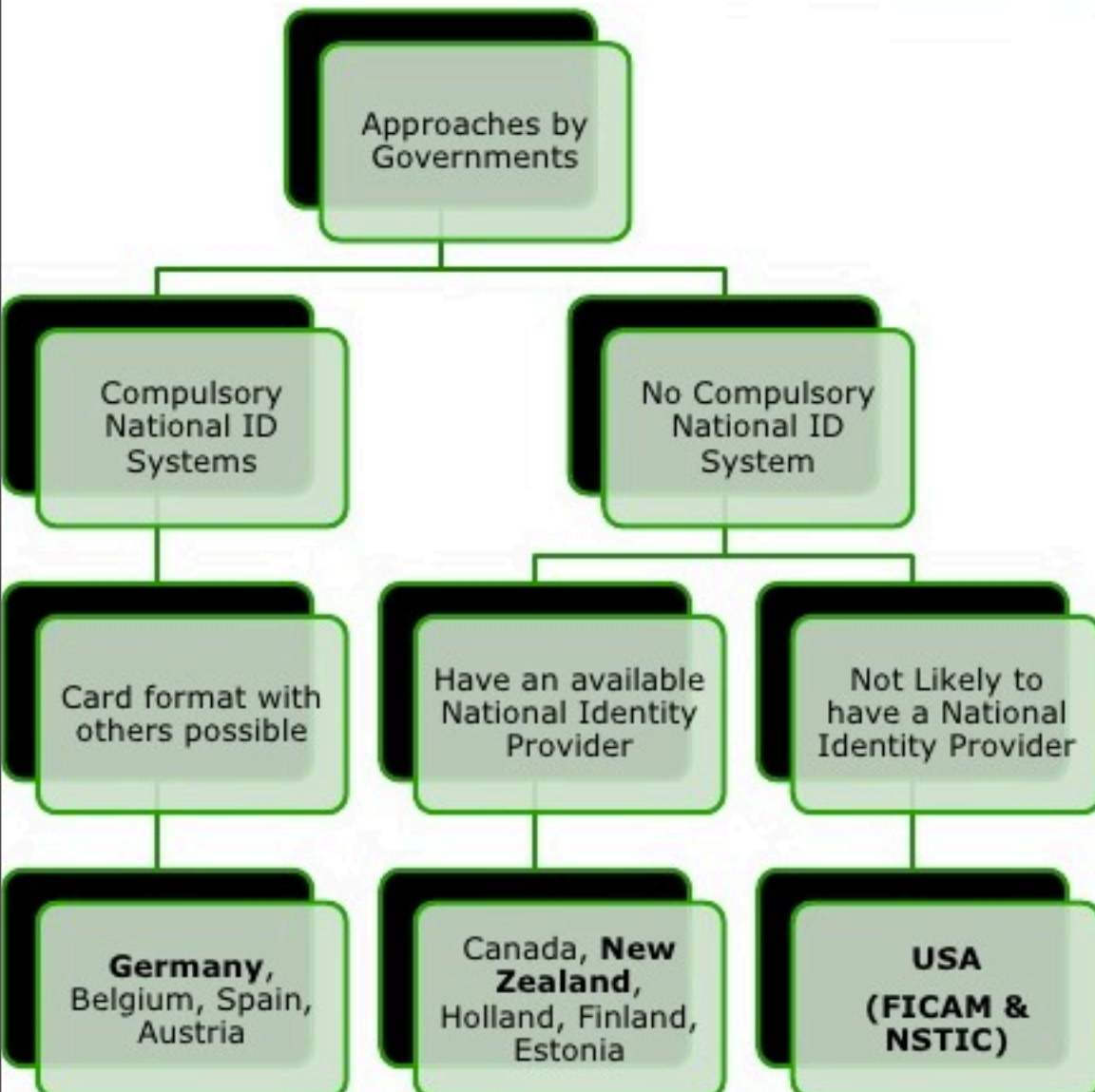
National Strategy for Trusted Identities in Cyberspace



eRecognition

Portalverbund - The Austrian Trust Federation

Comparison of Government Approaches



*Gardiner - EID conf



NIST & Stork - Authentication Assurance

- Government provided -NIST & Stork Level - one to one map

Table 2-1. Four Assurance Levels

Level	Description
1	Little or no confidence in the asserted identity's validity
2	Some confidence in the asserted identity's validity
3	High confidence in the asserted identity's validity
4	Very high confidence in the asserted identity's validity

- Idps and promote assurance level towards relying parties and end users, but need to be based on some independent verification.



Federation in Higher Education as a Testbed

- Educational - refeds.terena.org
 - REFEDS has been an open group working on the inter-federation issues for several years, but the work is changing pace as the federation work goes from identity deployment phase to federated identity being the preferred way of integrating your services. More services are moving into the federated identity layer, instead of using local user accounts.
 - global listing and survey of identity federations in higher education by country
 - includes hundreds of IDPs
 - Should be held as example implementation / proving ground for enterprise and public cloud identity initiatives



To do List - Identity Eco System

- Interoperability - start with Open standards - initially a single and later compliance with many
- Experience tells us that no single approach can address all of the use cases, security levels, levels of convenience, etc. so flexibility will be the killer app
- Provide mechanism to support Anonymity - implementation zero knowledge proof and other privacy enhancing technologies
- Taxonomy / Syntax across heterogeneous providers
- Audit for compliance and accountability
- The ecosystem will likely be varied and diverse with users still retaining more than one IDP, which means that users will need to manage divergent suppliers, and portability of identities becomes crucial
- Cornerstone - User Centricity maintenance across Trust frameworks
 - the fine print / Ts & Cs
 - equip users to make the right decisions
 - societal pressure - sign away user consent for functionality

- Schneier -Cryptogram
 - “Today we need to trust more people than ever before, further away -- whether politically, ethnically or socially -- than ever before. We need to trust larger corporations, more diverse institutions and more complicated systems. We need to trust via computer networks. This all makes trust, and inducing trust, harder. At the same time, the scaling of technology means that the bad guys can do more damage than ever before. That also makes trust harder. Navigating all of this is one of the most fundamental challenges of our society in this new century.”



Thank You.